
Commonwealth of Pennsylvania

Commonwealth Application Certification & Accreditation: (CA)²

2009 NASCIO Recognition Awards
Information Security

June 3, 2009

Summary

Like many organizations, the Commonwealth of Pennsylvania is shedding its hierarchical mainframe driven environments and embracing web-based technologies. We are transitioning from closed system, agency-centric modalities to an open, web-based environment which allows us to provide more services and data to our citizens and agencies. Drivers license processing and criminal history checks are just two examples of services that have migrated to web technologies over the past decade.

This paradigm change introduces security risks. In opening its services and data repositories to the Internet, the commonwealth had to consider SQL injections, cross site scripting (XSS), sensitive data leakage, cardholder data, PII, HIPAA and more.

To address such risks, the commonwealth launched *Operation Secure Enterprise* (OSE) which focused on network web-based threats. Unfortunately, over time hackers and crackers were able to bypass these security measures by changing from network-oriented to application-based attacks that exploit code vulnerabilities.

As these attacks increased, the Office of Administration, Office for Information Technology (OA/OIT) realized a need to change its security strategy from a network-centric model to a holistic model that includes application security. The result of which became the *Commonwealth Application Certification & Accreditation (CA)²* process.

(CA)² considers all OSI security layers by having agencies complete risk assessment questionnaires, source code scans, host based intrusion scans, and vulnerability assessments.

(CA)² has identified critical vulnerabilities that—if not corrected—could have been exploited, leading to identity theft and the propagation of malicious code. By closing such vulnerabilities before they are exploited, the commonwealth has prevented data leakage, identity theft, and theft of services and saved \$31.5 million dollars.

Description of the Problem

On January 4, 2008, the Commonwealth of Pennsylvania had to take several web applications offline for several hours because of a SQL injection that originated from China. Forensic examination of the server and database revealed that the hacker bypassed the application's security.

The attack modified 40+ tables with malicious entries. The intent was to embed URLs into commonwealth web sites so that users who unknowingly clicked on them were re-directed from the commonwealth site to a download which gave the hacker administrative rights to their personal PCs.

The commonwealth decided to restore impacted tables to a date before the attack occurred—which meant that the commonwealth, again, had to take all applications impacted by the attack offline.

Needless to say, the temporary loss of citizen services—including some that generate revenue; intervention required by commonwealth executives, lawyers and program experts; media scrutiny; and the suspension of other IT activities to solve this single problem were considerable.

Given the significant impacts, it was clear that the commonwealth needed to determine how vulnerable it was to these types of attacks. Thus, we began white hat hacking to assess our risk. The results of which showed that:

- there were an unacceptable number of applications susceptible to SQL injection attacks.
- there was a need to proactively evaluate web applications for compliance with commonwealth's policies, procedures, and standards to reduce potential SQL and XSS vulnerabilities.
- the commonwealth could save millions of dollars in costs associated with potential breaches.

In fact, of the approximately 50 applications selected at random, 24 had vulnerabilities significant enough to require immediate correction. Two were so significant that they exposed more than 350,000 sensitive records, which—according to minimum Gartner figures—could have cost the commonwealth \$31.5 million.

The commonwealth researched several risk assessment models and decided to create its own process based on the National Institute of Standards and Technology's special publication *800-37 Guide for the Security Certification and Accreditation of Federal Information Systems*. We removed federal policy, standard and authorization language and re-engineered the process to fit the commonwealth's system development life cycle. In so doing, we began building security controls into applications as they are being developed, rather than trying to apply security tools after-the-fact.

Since being implemented in May 2008, the (CA)² process has significantly reduced the number successful XSS and SQL attacks on the commonwealth's web applications. The (CA)² process has also saved the commonwealth millions of dollars in avoidance and soft costs associated with data breaches, remediation, and risk mitigation.

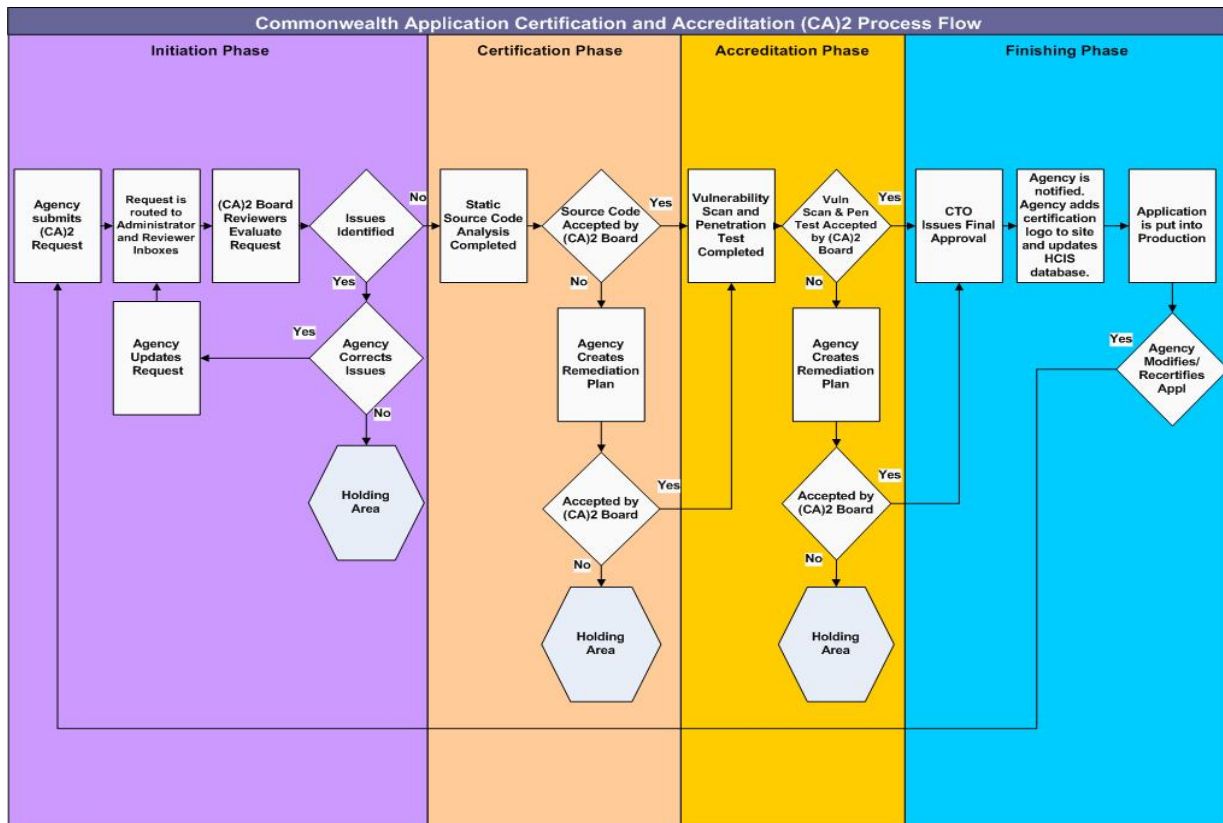
Significance of this project

The significance of (CA)² process can be measured in the results it has achieved. Since May 2008, the (CA)² process has:

- saved the commonwealth an estimated \$31.5 million in costs associated with potential breaches.
- significantly reduced the numbers of successful XSS and SQL inject attacks by proactively scanning web facing applications for XSS and SQL vulnerabilities.
- proactively integrated security controls into all phases of the commonwealth's system development life cycle.

(CA)² Solution and Benefits

The (CA)² Process consists of four phases: Initiation, Certification, Accreditation, and Finishing.



Initiation – Initiation consists of a policy compliance and risk assessment questionnaire to review new and existing web applications to determine if they comply with the commonwealth’s policies, procedures, and standards. The questionnaire is not cumbersome, it only takes an agency about 45 minutes to complete. Its value lies in the collection of pertinent data in a single location—IPs and points of contact are documented along with technical details, for example. Once completed, it is submitted to a team of enterprise architects and security analysts known as the (CA)² Review Board.

The review board determines if there are any risks that are not addressed in the applications security architecture. If so, the board will ask the agency to identify how they will address such risks before the application can proceed to certification.

Benefit – This process occurs at the beginning of the system development life cycle, so many production/security issues previously experienced by the commonwealth are being identified *before development begins*. This translates to millions of dollars of savings from potential breaches and remediation efforts.

Certification – During certification, agencies are required to conduct source code scans on their applications and the send results to the commonwealth. The commonwealth reviews reports and—based on finding—will require the agency to correct or approve the application to move forward in the process.

Benefit – Certification allows the commonwealth and agencies to detect application security risks, design flaws, policy violations, and common coding errors. In addition to validating compliance with the commonwealth’s development standards, certification compares applications to NIST and Open Web Application Security Project software vulnerability categories to provide a complete picture of potential risk that an application may pose.

Open source code testing:

- detects source code vulnerabilities before an application is put into production
- reduces testing and quality assurance costs for web application development by identifying issues before they are discovered by end users and hackers
- reduces help desk calls by identifying and correcting coding errors before they are discovered by end users
- shortens remediation by identifying code errors for developers to correct
- provides summaries and technical reports for benchmarking purposes

Accreditation – Prior to deployment, agencies are required to conduct vulnerability assessments on web servers and applications. The results from these scans are then submitted to the commonwealth for review to ensure that servers have the most current security patches and that the application is not susceptible to application layer attacks that may have been missed by the source code scan.

Benefit – Accreditation detects holes in web applications by using vulnerability assessment and penetration tools to scan the agency web servers and applications. The accreditation phase:

- confirms that the web server and application security functionality is in place and working correctly
- validates agencies server patch compliance with commonwealth standards
- simulates hacking techniques to identify and correct potential issues before the application is placed in production
- tests web applications for access to backend data via SQL injection and remote file inclusion techniques
- pinpoints exploitable OS vulnerabilities in network and endpoint systems
- distinguishes real threats from false positives to expedite remediation efforts
- saves millions in soft costs by identifying critical issues and prioritizing resolutions

Finishing – Finishing occurs prior to deployment and validates that nothing has changed in the application since it was first submitted. As part of this process, the agencies have to review their initial assessments. If there are no changes, the agency is given approval to place the application into production.

Benefit – Finishing validates the process that the architectural design has remained constant or, if changes have been made, they will not negatively impact security. In addition, the finishing phase ensures that applications will be placed in production environments that meet the commonwealth's IT policies, procedures, and standards and that all stakeholders are aware of the applications that are going into production.

Return on Investment

(CA)² has been tremendously successful in identifying potential flaws in web applications which could have led to breaches. All told, the commonwealth invests approximately 11 hours and agencies invest approximately five hours (or roughly \$800 in total staff time) per application. Estimated commonwealth savings from this process is in the millions of dollars.

Since its inception, approximately 1/3 of the applications submitted to the (CA)² process have revealed vulnerabilities that could have lead to breaches with the potential to cost the commonwealth millions of dollars. Positive outcomes from proactive web application scanning and white hat hacking efforts include:

- In May 2008, during a scan of a legacy application, a SQL vulnerability was discovered and remediated before the application went back into production. If the application hadn't been screened via (CA)², 150,000 records—containing employees' names, social security numbers, addresses and other data elements covered by the Pennsylvania Breach of Personal Information Act—may have been compromised by SQL inject.

- In June 2008, it was determined that a recently updated web application had a SQL vulnerability that would have exposed over 200,000 sensitive records. This vulnerability was identified by (CA)² and the agency corrected the issue before the application went into production.

The commonwealth is currently applying the (CA)² process to about five applications per month. We believe so firmly in our success that we built it into an open source web application to streamline/automate the process for our own state agencies and for other states to use. The application contains all of the questionnaires and assessments; coordinates the efforts of the review board; organizes attachments and reports; and provides a mechanism for dialog between the review board and the agency.

Government entities can download the source code at <http://www.cybersecurity.state.pa.us>. The site also contains descriptive materials, installation instructions, video, and database.