COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT'S OF PUBLIC WELFARE, INSURANCE AND AGING

INFORMATION TECHNOLOGY STANDARD

Name Of Standard: **Web Application Vulnerability Assessment Standard**	Number: **STD-ENSS034**
Domain: **Security**	Category:
Date Issued: **09/07/2012**	Issued By Direction Of:
Date Revised: **01/24/2014**	Shirley A. Monroe, Dir of Div of Technical Engineering

Abstract:

The purpose of this standard is to describe the minimum expectations for web application security vulnerability assessment and mitigation within the Commonwealth of Pennsylvania's Departments of Public Welfare, Insurance and Aging ("Departments").

As network and transportation layer security have matured, application layer attacks have increased exponentially. Recent years illustrate that web application vulnerabilities have outnumbered network layer vulnerabilities, fueling the urgency to secure custom-built web applications developed for the Department. Regulations such as Health Information Portability and Accountability Act (HIPAA), Internal Revenue Service (IRS) publication 1075 standard, and the Commonwealth's Data Breach Notification Acts drive the need to better secure web applications and to assess vulnerabilities before applications are deployed in a production, or a public-facing environment. In order to protect these systems, threats and vulnerabilities must be identified, assessed for the risks they pose and the findings reported to the Departments' Chief Information Security Officer (CISO) for timely remediation.

The web application security vulnerability assessment helps identify vulnerabilities within web applications custom code developed for the Departments only, and provides technical recommendations/mitigation steps to control the vulnerabilities before the applications are deployed production, or public-facing environments. This standard complements other vulnerability testing standards already in place within the Departments; however, the scope of this standard does not include infrastructure vulnerability testing[1]. The following activities are to be performed to improve web application security posture:

Scoping and Planning
This activity helps the Departments' Security Architecture Team gain perspective of the web application and/or code being assessed in order to derive the most applicable plan to complete the assessment.

Secure Code Review
A review of the web application source code aiming to identify insecure coding practices and document identified vulnerabilities.

Web Application Vulnerability Testing
A series of controlled application environment tests used to identify potential external security exposures and to evaluate the security posture of a web application. These tests are performed from both the non-user and end-user perspectives. The objective is to identify inherent weaknesses in the application design, implementation, and security controls from an application user/end user perspective.

Vulnerability Analysis, Mitigation Planning and Reporting
Analysis of any findings is conducted and a report is prepared that provides a listing of all vulnerabilities identified, risk ratings and remediation measures. This activity provides the CISO with the information needed to take the appropriate action to reduce and mitigate the risks posed to the Departments' public-facing environment and underlying network infrastructure.

Security Risk Assessment
A security risk assessment is conducted by the responsible representative for the underlying web application and the submission of a security risk self-assessment questionnaire. Please refer to the Departments' Risk Management Standard[2] for additional details on this activity.

General:

The Web Application Security Assessment Standard applies to the Departments' custom web applications developed internally or by contracted solution providers. The requirements outlined in this document are the minimum considered adequate to identify potential vulnerabilities due to insecure coding practices, insufficient design, and inadequate security controls during development of custom applications and code. The custom applications in scope of secure code review and vulnerability assessment include web applications, mobile web and mobile applications developed and/or purchased by and/or for the Departments.

Standard:

The Departments conduct both a secure code review and web application vulnerability testing during the Development (DEV) and Systems Acceptance Testing (SAT) phases of the Software Development Methodology (SDM) for any custom-developed web application being implemented under an initial system release, a subsequent release introducing new interfaces and/or business/data-access layer enhancements, or as determined by the Departments' CISO.

In addition, the Departments establish a baseline of the security posture of the applications once every three (3) years. As part of the baseline assessment, secure code review, vulnerability testing, analysis and a security risk assessment as outlined in this standard should be performed on any web application, including related services, that has not fallen within scope of a web application vulnerability assessment within the three (3) prior years.

The scope of this standard is limited to the custom code developed for the Departments only. The assessment will be performed only in the non-production environments including DEV, Integration (INT), SAT, or like environments. The appropriate system owners shall

work with the CISO and/or staff to identify the systems for this assessment. All vulnerability assessments must be approved by the CISO.

Scoping and Planning
The scanning need, whether necessitated by the introduction or modification of web applications and/or modules or periodic review, will dictate the scope and depth of the scanning efforts required. Typically, the Security Architecture Team will request a brief meeting with the requesting application team in order to gain perspective of the target web application or component including, but not limited to its:

- Purpose
- Target audience, including users and roles
- Functionality provided
- Data types involved, i.e. PII, HIPPA, etc.
- Related applications/services

This information will enable the team to properly scope their scanning efforts ensuring all user roles, functionality, and application use-cases are properly assessed.

Secure Code Review
Secure code review should be performed during the DEV phase of SDM. Secure code reviews help identify insecure coding techniques and potential security vulnerabilities that could lead to security breaches and/or malicious activity within the Departments' infrastructure. This activity reinforces the need for development teams to adhere to secure coding principles and is intended to identify issues as early as possible in SDM. Secure coding principles include, but are not limited to the following areas:

- Input Validation
- Output Encoding
- Authentication and Password Management (Refer to the Departments' User Access Management standard[3] for accepted authentication standards)
- Session Management
- Access Control
- Cryptographic Practices
- Error Handling and Logging (Refer to the Departments' Audit Logging Policy[4] and Standard[5] for accepted logging standards)
- Data Protection
- Communication Security
- System Configuration
- Database Security
- File Management
- Memory Management
- Service Integration (Refer to the Departments' Services Security Standard[6])
- General/Overall

Please refer to the Open Web Application Security Project (OWASP) Secure Coding Practices Quick Reference Guide[7] for elaborations on those secure coding practices highlighted above. By enforcing secure coding practices, performing secure code reviews and vulnerability testing, the Departments are taking a proactive approach in ensuring that as few as possible vulnerabilities are deployed and that others are identified and assessed for later mitigation.

The Departments have established IBM AppScan Source Edition[8] as the standard secure code review tool. Application development team members and contracted support staff are expected to use the standard tools and perform the tests during the DEV phase of SDM. The

identified security vulnerabilities should be mitigated through necessary design and/or code changes and re-scanned via the standard secure code review tool to confirm before proceeding to the next phase of the SDM. Any exemptions requests must be submitted to the Departments' CISO for review and approval prior to proceeding with the next phase of he SDM.

Web Application Vulnerability Testing

Web application vulnerability testing should be performed during the SAT phase of SDM. This assessment helps identify the potential weaknesses in the design, implementation, and security controls of custom applications that may be present and relative to those development areas previously mentioned in the Secure Code Review section of this standard. The tests should be performed from the perspective of an (un-authenticated) attacker as an (authenticated) application end-user. The implications resulting from identified weaknesses should be documented against leading web application security standards such as outlined in previous sections of this standard. The testing is expected to be performed based on end-user perspectives at various roles within the enterprise.

The Departments have established HP WebInspect[9] as the standard web application security vulnerability scanning tools. Security Architecture Team members and contracted support staff are expected to use the standard tools and perform the tests during the SAT phase of SDM. The identified security vulnerabilities should be communicated to the CISO and mitigated according to the guidelines defined in the section "Vulnerability Analysis, Mitigation Planning and Reporting" or as defined by the CISO. Finally, the status of a completed secure code review and web application vulnerability tests, including identified vulnerabilities and mitigation status, should be communicated to the Departments' Architecture Review Board[10] for review and approval prior to proceeding with the next phase in the SDM.

Vulnerability Analysis, Mitigation Planning and Reporting

The results of the secure code review, application vulnerability assessment and security risk assessment should be shared with the Departments' CISO as soon as each of the tests is completed. Upon obtaining mitigation plan approval from the CISO, an integrated infrastructure security assessment report should be submitted including the following details:

- Security vulnerability/Risk Identifier
- Security vulnerability/Risk Category
- Security vulnerability/Risk Title
- Brief description of the Security vulnerability/Risk
- Potential business impacts
- Mitigation status
- Mitigation plan
- Date first reported
- Departments' approval status (Approved-Mitigated/Approved-Waiver Submitted/Unapproved)
- Departments' waiver status (Open/Closed/Expired)

It is expected that the security vulnerabilities or regulatory risks identified by the assessment activities are managed by the Program Office's application development team similar to any other application bugs, documented and addressed using the steps outlined below:

- Open a Bug attached to a work item in Team Foundation Server (TFS) 2010 when a vulnerability is identified

- Prioritize the resolution for each vulnerability based on severity (business impact)
- Identify the mitigation strategy for each critical and high severity Bug during the current release of the application
- Monitor the bug for timely closure
- Once fixed, re-validate with a repeat scan to confirm that the vulnerabilities no longer exist
- For any vulnerability that is not mitigated, the respective program office must submit a security risk acceptance request to the CISO using the Departments' IT Risk Management (ITRM) solution. This request should be placed during the integration test phase of Software Development Methodology
- Obtain risk acceptance (if required) from the CISO and monitor the Bug for timely closure

In addition, the appropriate team should perform a business impact analysis for the identified vulnerabilities and security risks. The report detailing the vulnerabilities, security risks, the security severity, business impact and the corresponding mitigation plan should be submitted to the CISO. Upon consensus of the vulnerability mitigation plan, the mitigation plan should be documented and managed by the program office similar to other application defects.

Security Risk Assessment

The Departments have established an IT Risk Management (ITRM) to assist their efforts of continuously monitoring the regulatory compliance posture of the information technology assets. As part of this effort, the Departments require the appropriate program office representative to conduct a security risk assessment and submit a security risk self-assessment questionnaire on the network infrastructure. Through the recurring assessment process, the Departments should:

- Update the list of known vulnerabilities at least quarterly or when new vulnerabilities are identified and reported
- Pro-actively determine trends related to infrastructure vulnerabilities to ensure policies, standards and/or procedures are up to date in the efforts to eliminate or reduce future vulnerabilities

The security risk self-assessment questionnaire should be submitted using the Departments' ITRM solution. The submitted self-assessment questionnaire will be reviewed by the Departments' Security Architecture Team to identify potential security, regulatory risks, and advise on mitigation planning going forward. Please refer to the Departments' risk management standard[4] for details on conducting this activity.

Exemptions from this Standard:

Any exemptions to comply with this standard should be discussed with the Departments' CISO.

Refresh Schedule:

All standards and referenced documentation identified in this standard will be subject to review and possible revision annually or upon request by the Departments' Information Technology Standards Team.

Standard Supplements:

None

References:

1. STD-ENSS028: Infrastructure Vulnerability Assessment (http://mydpw.dpw.state.pa.us/cs/groups/webcontent/documents/communication/p_031984.pdf)
2. STD-ENSS031: Risk Management (http://mydpw.dpw.state.pa.us/cs/groups/webcontent/documents/communication/p_031988.pdf)
3. STD-ENSS033: User Access Management (http://mydpw/cs/groups/webcontent/documents/communication/p_031990.pdf)
4. POL-SEC009: Security Audit Logging Policy (http://mydpw.dpw.state.pa.us/cs/groups/webcontent/documents/communication/p_031975.pdf)
5. STD-ENSS026: Audit Logging (http://mydpw.dpw.state.pa.us/cs/groups/webcontent/documents/communication/p_031981.pdf)
6. STD-ENSS032: Services Security (http://mydpw.dpw.state.pa.us/cs/groups/webcontent/documents/communication/p_031989.pdf)
7. OWASP Secure Coding Practices Quick Reference Guide (https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf)
8. IBM AppScan Source Edition (http://www-01.ibm.com/software/rational/products/appscan/source/)
9. HP WebInspect (http://www8.hp.com/us/en/software-solutions/software.html?compURI=1341991&jumpid=reg_r1002_usen_c-001_title_r0001)
10. Architecture Review Board (ARB) (http://mydpw/oa/bis/busandtechstandards/arb/index.htm)

Standard Revision Log:

Change Date	Version	Change Description	Author and Organization
09/07/2012	1.0	Web Application	Clifton Van Scyoc
10/24/2013	1.1	Secure Code Review	Mathieu Saury
01/24/2014	1.2	Standard update	Christopher Kajder