8-605. Web applications and services.

Internet-facing systems are diverse to meet a multitude of different needs. Therefore, information exposures by these systems differ, as do threats. Security controls should be implemented to mitigate meaningful risks to an application. Because every system is different, the web application developer is the most knowledgeable about the system and the risks it faces.

This standard establishes a baseline of security requirements for all state websites, web services, and all vendor supported or hosted web applications. All applications that are Internet-facing are required to securely maintain documentation and evidence of compliance levels with this standard.

This standard is based on the research and recommendations from the SysAdmin, Audit, Network, and Security (SANS) Institute and the Open Web Application Security Project (OWASP). The following are the security standards for web applications and services:

(1) Consider the threats, vulnerabilities, and risks to your application. If you are unsure, follow the threat risk methodology published by OWASP (http://www.owasp.org/index.php/Threat_Risk_Modeling);

(2) Consider and implement additional security controls to ensure the confidentiality, integrity, availability of the information based on the unique threats and exposures that face your application;

(3) Implement error-handling in a manner that denies processing on any failure or exception;

(4) All input fields must be validated before accepting. Input should be checked to prevent the program from executing malicious code. Input length must be validated to determine if it is within the predetermined minimum and maximum ranges. Input values should be screened for valid data types (e.g., number or character only, no special characters);

(5) Output fields must be sanitized to ensure the output does not reveal too much information that could be used by malicious intent (e.g., default system-generated messages should be translated by the application). If invalid user input is encountered, the error message should not reveal the specific component which caused the error. Messages should be general in nature, and not reveal anything more than what is necessary;

(6) The identity of the user must be authenticated if the application has access to non-public information. All user credentials and passwords must meet the security policy requirements for strength, change, and history. User access and capability must be limited to the functions required for the authorized access level only;

(7) The requesting and granting of user accounts must include an approval process that validates the user and the minimum necessary access levels;

(8) Establish security settings commensurate with the type of access;

(9) All external systems (including web services), which require access to the application, must be authenticated and permissions checked before the external system becomes trusted;

(10) All password entry fields should not "echo" the password in readable text when it is entered. Auto-complete of password fields should be disabled;

(11) All sessions should be terminated when the user logs out of the system;

(12) If a web application needs to store temporary or session-related information that is CONFIDENTIAL or RESTRICTED outside of the secured agency internal network, that information must be encrypted in all cases – whether stored or in transit. Encryption technology must be approved by Office of the CIO;

(13) All web applications are required to have a security scan and test of the application on a recurring basis as determined by the state information security officer. Higher risk or impact applications should be tested annually. This test shall be coordinated and supervised by the state information security officer, agency information security officer, and IT management. Some packaged web applications where the package's architecture inherently protects the application from security risks, may have reduced testing requirements versus other web applications; and

(14) The anonymous public facing environment shall contain publicly approved content only. All non-public data and applications shall be segregated by additional firewalls and network monitoring.

[Other application security recommendations and development guides can be reviewed at the OWASP (https://www.owasp.org/index.php/Category:OWASP_Guide_Project) and SANS (http://www.sans.org/top25-software-errors/) websites.]

--

History: Adopted on July 12, 2017.
URL: http://nitc.nebraska.gov/standards/8-605.pdf