UF UNIVERSITY of FLORIDA
Health Science Center

Security Program for the Information and Computing Environment

Standard

Standard: TS0011.03	Category: Technical Security	Version Date: 2/15/2008
Title: Web Application Security		Effective Date: 4/1/2008
Originating Unit: Security Program for the Information and Computing Environment Project		Last Review: 2/15/2008
Review Resp: HSC Chief, Information Security		Next Review: 2/2010

Purpose:

To provide a source of recommended security controls for web applications.

References:

1. SPICE Policy TS0011 Software Security Compliance.
2. UF Guidelines to Develop Applications for Secure Deployment. http://www.it.ufl.edu/policies/guidelines.html
3. Open Web Application Security Project http://www.owasp.org/index.php/Main_Page
    a. Principles http://www.owasp.org/index.php/Category:Principle
    b. Countermeasures http://www.owasp.org/index.php/Category:Countermeasure
4. Web Application Security Consortium http://www.webappsec.org
5. SPICE Evaluation Program
    a. Products and Services Security Evaluation Procedures
    b. EV0001 – Information Technology Products and Services Security Evaluation Form

https://security.health.ufl.edu/isa_ism/eval_artifacts.shtml

Standard:

1. Web Application Security Awareness – All HSC staff or contractors *developing custom web application software* for installation on HealthNet or for HSC use must familiarize themselves with the following web application security principles.
    a. Principles (see OWASP Principles for definitions):
        i. Apply defense in depth (complete mediation)
        ii. Use a positive security model (fail safe defaults)(minimize attack surface)
        iii. Fail safely
        iv. Run with least privilege
        v. Avoid security by obscurity (open design)
        vi. Keep security simple (verifiable)(economy of mechanism)
        vii. Detect intrusions (compromise recording)
        viii. Don't trust infrastructure or external services
        ix. Establish secure defaults
2. Web Application Security Countermeasures – The following web application security countermeasures *must be addressed* in web application design, development and enhancements of *custom web application software* for installation on HealthNet or for HSC use:
    a. Countermeasures (see OWASP Principles for definitions):

i. Access Control
ii. Authentication
iii. Canonicalization
iv. Cryptography and encryption
v. Encoding
vi. Error Handling
vii. Input Validation
viii. Logging
ix. Mechanism
x. Quotas
xi. Session Management
xii. Validation

3. To minimize host compromise through web applications, *all web application software, including commercial, open source, or custom written*, to be installed on HealthNet *must be tested*:
    a. for error handling, input validation and session management,
    b. using manual testing or automated mechanisms or a trusted 3rd party (i.e. certifying agent) with the results saved and available upon request.
4. The security features listed above are elaborated in the SPICE products and services security evaluation process and procedures which should be performed prior to resource investment (i.e. buying a product, expending integration effort, or writing code) in new software or software services. The procedures and evaluation form are in the references above.
5. The recommendations generated from the security evaluation must be completed prior to use of the software on production systems, prior to use by users and prior to interaction with Restricted or Sensitive information unless otherwise stated in the evaluation report.