Institutional Compliance
Office of Information Security

OIS 37 – Standard for Web Application Vulnerability Scanning

I. STANDARD STATEMENT

Good application security consists of knowledge of threats and regular feedback on the state of protection within an application.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

informationsecurity@utsa.edu

V. PROCEDURES

A. Business units and system administrators must be aware of the vulnerabilities that can exist within the applications so that appropriate actions can be taken to mitigate these risks. Vulnerability scanning is a procedure designed to identify security weakness in the application and to assist in mitigation of those weaknesses.
B. All Web applications attached to the UTSA network are subject to security vulnerability scans. Proactive scanning allows for timely discovery of known risks and promotes actions to prevent compromise, breach and destructive activity within application and/or the network. Reactive security scanning provides a means of assessment and damage control. Coordinate with OIS for a vulnerability scan.
C. Scans are required:
    1. Prior to the promotion to production of a Web application associated with a formal project.
    2. After a compromise of a UTSA Web application accessible through the Internet.
    3. Annually for all mission-critical operations.
    4. Other Web applications will be scanned at the request of the application owner when potential or existing risks are identified within the environment.

Title: OIS 37 – Standard for Web Application Vulnerability Scanning
Effective Date: April 22, 2012
Last Reviewed: August 13, 2020