
Web and E-Commerce Security [1]

Topics:

[access](#) [2], [physical access](#) [3], [logical access](#) [4], [authorization](#) [5]

SS-08-049 Web and E-Commerce Security

Issue Date: 3/31/2008

Effective Date: 3/31/2008

PURPOSE

The World Wide Web (i.e. the ?Web?) also known as the Internet, is one of the most beneficial resources for publishing an organization?s information, interacting with constituents and businesses and establishing an e-commerce/e-government presence. However, if an organization is not rigorous in configuring and operating its public website, it may be vulnerable to a variety of security threats. Web servers are often the most targeted and attacked hosts on organizations? networks. As a result, it is essential to secure web servers and the network infrastructure that supports them.

This standard establishes the minimum security measures each agency must implement on public access, web facing systems.

STANDARD

All agencies shall properly plan for and address information security requirements prior to deploying an internet based web server and/or web services.

Agencies shall:

- Have a secure network infrastructure that physically allocates publicly accessible information system components (e.g., public web servers) to separate sub-networks, each of which will have separate, physical network interfaces and prevents public access into the organization?s internal networks (e.g. DMZ).
- Standardized secure operating system and application configurations, deployment and maintenance strategies.
- Ensure that web application developers and web masters design using security engineering principles in accordance with guidance provided in NIST SP 800-27 Engineering Principles for Information Technology Security.
- Establish policy and processes to ensure that only appropriate/authorized web server content is published and accessed.
- Limit user activity that does not require identification and authentication, and implement authentication and cryptographic technologies as appropriate to meet data security/privacy requirements.

- Perform logging and implement controls to prevent, monitor and respond to unauthorized modifications to web server content and applications, intrusions, malicious code, system failure or other forms of compromise.
- Be Payment Card Industry Data Security Standard (PCI DSS) compliant when providing on-line customer payment processing services or shall validate the PCI compliance of third-party service providers outsourced to store, process, or transmit credit card data on their behalf.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

[Public Access Systems \(PS-08-028\)](#) [6]

[Network Security-Information Flow \(PS-08-030\)](#) [7]

[Network Access Controls and Session Controls \(SS-08-048\)](#) [8]

[Network Security-Boundary Protection \(SS-08-047\)](#) [9]

REFERENCES

NIST SP 800-44 Guide for Securing Public Web Servers

NIST SP 800-96 Guide to Secure Web Services

NIST SP 800-27 Engineering Principles for Information Technology Security

NIST SP 800-28 Guidelines for Active Content and Mobile Code

NIST SP 800-52 Guideline for Selection and Use of Transport Layer Security Implementation (SSL)

PCI Data Security Standard, see <https://www.pcisecuritystandards.org/> [10]

TERMS and DEFINITIONS

Controlled Interfaces - Mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system such as but not limited to proxies, gateways, routers, firewalls, encrypted tunnels).

Demilitarized Zone (DMZ) - A host or network segment inserted as a "neutral zone" between an organization's private network and the Internet.

Web Server - A computer that provides World Wide Web (WWW) services on the Internet. It includes the hardware, operating system, Web server software, and Web site content (Web pages). If the Web server is used internally and not by the public, it may be known as an "intranet server."

Webmaster - A person responsible for the implementation of a Web site. Webmasters should be proficient in HTML and one or more scripting and interface languages, such as JavaScript and Perl. They may or may not be responsible for the underlying server.