

GUIDELINES AND INFORMATION RESOURCES FOR SECURING PUBLIC WEB SITES OF HEALTH DATA ORGANIZATIONS

OCTOBER, 2004

PREPARED BY

WALTER G. SUAREZ, MD, MPH
MIDWEST CENTER FOR HIPAA EDUCATION



TABLE OF CONTENTS

INTRODUCTION 1

BASIC PRINCIPLES FOR SECURING PUBLIC WEB SITES 2

WHAT THIS DOCUMENT DOES NOT COVER 2

WEB SECURITY CORE COMPONENTS 3

WEB SERVER SECURITY 3

CONFIGURING WEB SERVER TECHNOLOGY 4

MAINTAINING WEB SERVER INTEGRITY 8

WEB SITE SECURITY 10

WEB SECURITY CHECKLISTS 14

APPENDIX A - GLOSSARY

APPENDIX B - RESOURCES

NATIONAL ASSOCIATION OF HEALTH DATA ORGANIZATIONS

Guidelines and Information Resources for Securing Public Web Sites of Health Data Organizations

Prepared by
Walter G. Suarez, MD, MPH
Midwest Center for HIPAA Education
~ October, 2004 ~

INTRODUCTION

The Internet is one of the most cost-effective and efficient ways for health data organizations to collect, aggregate and publish health information, interact with health data suppliers and users, and establish an e-commerce business presence.

However, if the organization is not rigorous in securely configuring and operating a public Web site, it leaves itself vulnerable to a variety of information security problems that affect the integrity, availability and confidentiality of the health information.

Insecure and compromised Web sites serve as the entry point for intrusions into an organization's internal networks for the purpose of accessing non-public, confidential information. In addition to the risk posed to the individuals that are the subject of the data, the organization is exposed to elevated levels of liability risks and business losses.

The purpose of this document is to assist health data organizations develop and adopt best practices and policies that ensure that their public Web sites are a safe and secure environment for the collection, use and dissemination of health information.

The practices recommended below are designed to help health data organizations mitigate the risks associated with these and several other known security problems. They do not cover the implementation of practices for securing network servers and internal networks. The organization needs to ensure that it first configures a secure general purpose server within a secure network environment before tailoring its configuration to operate as a public Web server.

BASIC PRINCIPLES FOR SECURING PUBLIC WEB SITES

- The organization wants to maintain the integrity of all information resident on and accessible via their Web site.
- The organization wants to protect the confidentiality of all information resident on and accessible via their Web site.
- The organization wants to ensure the availability of certain portions of the information resident on and accessible via their Web site.
- The organization wants to prevent the use of their Web host as a staging area for intrusions into the organization's network that could result in breaches of confidentiality, integrity, or availability of information resources.
- The organization wants to prevent the use of the Web host as a staging area for intrusions into external sites, which could result in your organization being held liable for damages.

WHAT THIS DOCUMENT DOES NOT COVER

This document is not intended to provide advice that will cover all possible website implementations by health data organizations. Rather, it is the responsibility of the organization to ensure that their website implementation complies with a minimum number of guidelines and requirements that protect the integrity, availability and confidentiality of the information being provided via their Web sites. In particular, they do not address:

- Securing a general purpose network server. Practices to accomplish this are outside of the scope of this document.
- Firewalls and routers used to protect Web servers.
- Security considerations related to Web client (browser) software
- Commercial transactions via the Web (with the exception of a brief description of Secure Electronic Transaction [SET])
- Special considerations for very large Web sites with multiple hosts
- Contracting for or offering Web-hosting services (such as those provided by a commercial Internet service provider)
- Other public information services, such as those based on the file transfer protocol (FTP)
- Privacy protection and anonymity, specifically protecting personal identify and preferences that are available to Web servers (such as name, location, computer used, browser used, last URL visited)
- Protection of intellectual property

WEB SECURITY CORE COMPONENTS

Web security can be broken down into at least two logical subdivisions - the security of the Web server itself and the security of the sites on the server. Other factors like the security of the network on which the Web server resides are not covered in this document.

A. Web Server Security

There are three main security issues related to the operation of a public Web server:

1. Improper configuration or operation of the Web server can result in the inadvertent disclosure or alteration of confidential information. This can include:

    - information assets of the organization
    - information about the configuration of the server or network that could be exploited for subsequent attacks
    - information about who requested which documents from the server
    - sensitive customer or user information

2. The host used for your Web server might be compromised. This could allow intruders to:

    - change the information stored on the Web server host machine, particularly the information you intend to publish
    - execute unauthorized commands or programs on the server host machine including ones that the intruder has installed
    - gain unauthorized access to resources elsewhere in your organization's computer network
    - launch attacks on external sites from your server host machine, thus concealing the intruders' identities, and perhaps making your organization liable for damages

3. Users can be unable to access the organization's Web server if all of its resources are consumed by a denial-of-service attack.

Specific methods for securing a web server largely depend on the operating system (OS) and Web server software used. The vast majority of Web servers run either **Apache** or **Internet Information Server (IIS)** Web server

software. Apache can run on the Windows platform, but usually runs on Linux or some other flavor of Unix. IIS runs on the Windows server platforms.

Following are the recommended practices related to securing a Web server in health data organizations. They are organized into two main categories: 1) configuring Web server technology and 2) maintaining Web server integrity.

CONFIGURING WEB SERVER TECHNOLOGY

1. Isolate the Web server from public networks and your organizations internal networks

   A public Web server host is a computer intended for public access. This means that there will be many people who will access the host (and its stored information) from locations all over the world. Regardless of how well the host computer and its application software are configured, there is always the chance that someone will discover a new vulnerability, exploit it, and gain unauthorized access to the Web server host (e.g., via a user account or a privileged account on a host with a multiuser operating system). If that occurs, the organization needs to prevent these subsequent events, if possible:

   - The intruder is able to observe or capture network traffic that is flowing between internal hosts. Such traffic might include authentication information, proprietary business information, personnel data, and many other kinds of sensitive data.
   - The intruder is able to get to internal hosts, or to obtain detailed information about them.

   To guard against these two threats, the public Web server host must be isolated from your internal network and its traffic, as well as from any public network.

2. Configure the Web server with appropriate object, device, and file access controls

   Most Web server host operating systems provide the capability to specify access privileges individually for files, devices, and other data or code objects stored on that host. [1] Any information that your Web server can access using these controls can potentially be distributed to all users accessing your public Web site. Your Web server software is likely to provide additional object, device, and file

access controls specific to its operation. You need to consider how best to configure these access controls to protect information stored on your public Web server from two perspectives:

- To limit the access of your Web server software
- To apply access controls specific to the Web server where more detailed levels of access control are required

The proper setting of access controls can help prevent the disclosure of sensitive or restricted information that is not intended for public dissemination. In addition, access controls can be used to limit resource use in the event of a denial-of-service (DoS) attack against your public Web site.

3. Identify and enable Web-server-specific logging mechanisms

Log files are often the only record of suspicious behavior. Failure to enable the mechanisms to record this information and use them to initiate alert mechanisms will greatly weaken or eliminate your ability to detect intrusion attempts and to determine whether or not they succeeded. Similar problems can result from not having the necessary procedures and tools in place to process and analyze your log files.

As a general case, system and network logs can alert you that a suspicious event has occurred that requires further investigation. Web server software can provide additional log data relevant to Web-specific events. If you do not take advantage of these capabilities, Web-relevant log data may not be visible or may require a great deal of effort to access.

You may need Web server logs to:

- Alert you to suspicious activity that requires further investigation
- Determine the extent of an intruder's activity
- Help you to recover your systems
- Help you to conduct an investigation
- Provide information required for legal proceedings

4. Configure the Web server to minimize the functionality of programs, scripts, and plug-ins

Programs, scripts, and plug-ins (collectively referred to as external programs in this practice) can add valuable and useful functionality to an organization's public Web service. They are widely available from many different sources. Web administrators can add them to the Web server at any time without having to modify the server code. If the organization's Web service requirements can only be met through the use of external programs, the organization needs to thoroughly review and determine how these external programs will be configured, used, and administered. The goal should be to restrict their functionality to the greatest extent possible to keep potential security risks to a minimum.

When considering the functionality of programs, scripts and plug-ins, the organization should:

- Verify that the acquired copy of an external program is an authentic copy
- Scan all external programs for computer viruses and Trojan horses
- Exercise all acquired external programs on a test machine isolated from your internal network prior to operational use
- Execute tools and include mechanisms that limit the organization's exposure to vulnerabilities in external programs
- Mitigate the risk of distributing malicious code
- Disable or restrict the use of server side include functionality
- Disable the execution of external programs present in your Web server configuration
- Configure Web server host operating system and Web server software access controls to restrict access to external programs
- Ensure that only authorized users can access external programs
- Configure the Web server to execute external programs under unique individual user and group IDs
- Restrict the access of external programs to only essential files
- Create cryptographic checksums or other integrity-checking information for all external programs

5. Consider security implications before selecting programs, scripts, and plug-ins for your Web server

Security vulnerabilities can be easily introduced in the acquisition, installation, configuration, deployment, and operation of

programs, scripts, and plug-ins (collectively referred to as external programs in this practice). The Web server administrator may install a specific set of external programs that result in a unique configuration--one that has likely not been tested by the developers of your Web server software or the external programs. Vulnerabilities may include poorly written programs never intended for wide-scale use or unexpected side effects that are created when two or more programs are installed that were not intended to operate together. For example, many successful attacks on Web sites have exploited known vulnerabilities in commonly available CGI scripts.

When selecting programs, scripts and plug-ins, the Web administrator should consider:

- The functionality that each external program provides. Decide if it is important to have this functionality, or if it would just be nice to have but not essential.
- The external program's ease of installation, configuration, testing, and maintenance
- The potential security vulnerabilities introduced by the external program and the inherent risks to your public Web site
- The potential security vulnerabilities introduced by two or more external programs when used in combination

6. Take additional Web server protective and monitoring measures

- Keep OS Up to Date with Patches

  Always keep OS and web server software patched with the latest available patches. When setting up the OS, consider that the primary role of the server is a web server and look for specific OS configuration options that will enhance the security in this role.

- Shutdown Web Server or Disconnect from Network When Building or Updating a Web Server

  Always build a web server off of the network. Do not connect the web server to the Hopkins network until it is fully patched and updated. If you need to put the server on the network to download patches, shut off the web server component until the patching is done. It is best to assume that the web server will be constantly under attack from various exploits. It should only be placed on the

network when the safeguards for current known vulnerabilities have been put in place.

- Eliminate Unnecessary Services, Applications, Protocols, and Ports on a Web Server

  The general rule of eliminating unnecessary services is critical when hardening a web server. If possible, run other applications, like database engines, on separate servers. Eliminate as many unneeded protocols and open ports as possible. In particular, many web servers also run FTP servers or SMTP servers when they are not needed.

- Consider Disabling NetBios on a Web Server

  If running on the Windows platform, consider disabling all NetBios activity. The Server service can be shut down and not directly affect IIS. This prevents many non-web attachments to the server such as drive mappings.

- Maintain Access Logs

  Always make sure that the web server records access logs and that they are stored in a secure location on the web server, apart from the web-accessible files. Web server logs should include a minimum of time, date, remote client IP address, and resource requested. In the event of a security incident, log files are an essential tool for diagnosis.

MAINTAINING WEB SERVER INTEGRITY

1. Maintain the authoritative copy of your Web site content on a secure host

   The authoritative (i.e., verified, correct, trusted) copy of your public Web site content needs to be stored on a host that is separate from (and more secure than) your public Web server. The more secure host will likely be one that is on your internal network and protected behind one or more firewalls.

   If the integrity of the information on your public Web server is ever compromised, the organization can then restore it from the authoritative copy using a secure transfer procedure.

Organizations that rely on their Web sites to transact business must be able to quickly restore them to their authentic version; otherwise, they run the risk of losing business and customer confidence.

The authoritative copy of the organization's public Web site content is less likely to be compromised by an intruder if it is stored in a more secure location. As a result, it will likely be correct and available when you need to restore the publicly-accessible version.

In maintaining an authoritative copy of the organization's public Web site, the following should be considered:

- Restrict the number of users with access to the authoritative version of your public Web site's content
- Implement and enforce access controls at the level of Web content subdirectories
- Enforce the use of strong user authentication before granting access to the authoritative version
- Configure your public Web server to accept an authenticated and encrypted connection initiated by the secure host where the authoritative copy is stored
- Establish manual procedures to transfer the authoritative copy of the Web server content if you are unable to use a network

2. Protect the organization's Web server against common attacks

The organization must anticipate the occurrence of attacks and be prepared to deal with those directed against your public Web site. If these attacks are successful and you are not prepared, your organization may suffer the consequences of a defaced, inaccurate, or unavailable Web site. These could include being unable to conduct business and result in a loss of customer confidence and reputation.

Attackers can target

- the Web server host operating system
- Web server software
- programs, scripts, or plug-ins used by Web server software
- firewalls and routers that protect your public Web site and your internal network. This includes Internet Service Providers and other organizations providing network services.

Attacker objectives may include:

- gaining direct access to your Web server
- changing Web site contents
- denying user access to your Web server[1]

In protecting the organization's Web site against common attacks, the following should be considered:

- Regularly review publicly available information on recent security vulnerabilities and incidents
- Update your security controls to mitigate against new attacks and vulnerabilities
- Augment your alerting procedures
- Work with the organization's network provider to determine how the organization can mitigate damages due to distributed denial of service attacks

B. Web Site Security

Once the web server itself has been set up in as secure a manner as possible, it is time to consider the security of the sites which will be hosted on that web server. Web site security is more flexible than web server security; decisions made about the web server usually affect all the hosted sites, but decisions about web site security can be customized for each particular site. Web site security uses a combination of authentication and encryption methods.

Without strong user authentication, and organization will not be able to restrict access to specific information by authorized users. All information that resides on your public Web server will be accessible by anyone who accesses that server.

Without strong server authentication, users of the organization's public Web server are not able to determine if they have connected to an authentic Web server or a bogus version operated by an intruder. In such cases, the user may receive false information and act upon it based on the assumption that it originated from your Web server. The user may also provide sensitive information such as a credit card number.

Encryption can be used to protect information meshing the connection between a Web browser client and a public Web server. Without encryption, anyone with access to network traffic (accomplished via the use of a sniffer) can determine, and possibly alter, the content of sensitive and restricted information,

even if the user accessing the information has been carefully authenticated. This may violate the confidentiality and integrity of critical information.

When assessing the use of authentication and encryption technologies, the Web administrator should:

- Determine the access requirements for sensitive or restricted information that needs to be available via the organization's public Web server

- Understand the importance of establishing trust between clients (users) and Web servers

  External users (clients) need to be sure that:

  - they are communicating with the correct server
  - what they send is delivered unmodified
  - they can prove that they sent the message
  - only the intended receiver can read the message
  - delivery is guaranteed

  The Web server needs to be sure that:

  - it is communicating with the right client
  - the content of the received message is correct
  - the identity of the author is unmistakable
  - only the real author could have written the message
  - it acknowledges receipt of the message

- Understand the limitations of address-based authentication

- Understand authentication and encryption technologies and when each should be used. Based on the well-established standards, there are a limited number of technologies available to restrict access to information residing on a public Web site. These are:

  1. Basic Authentication

     This technology utilizes the Web server content's directory structure. Typically, all files in the same directory are configured with the same access privileges. A requesting user provides a recognized user ID and password for access to files in a given directory. More restrictive access control can be enforced at the level of a single file within in a directory, given that the Web server software provides this capability. Each vendor's

Web server software has its own method and syntax for defining and using this basic authentication mechanism.

Basic Authentication is supported by any standard-compliant Web browser.

2. Secure Socket Layer (SSL)

   SSL is composed of two sub-protocols called SSL record protocol and SSL handshake protocol. The handshake protocol is used to exchange any information about cryptographic capabilities and keys used. The record protocol is used to exchange the actual data.

   SSL uses public key cryptography. Certificate authorities can be used to verify the relationship between users and organizations. CAs can also be used to verify a specific user's relationship to specific server keys. Both of these verification actions allow users of the CA to have a higher level of trust in the relationships and the keys based on the user's trust in the CA and the CA's compliance with regulations directing their actions.

3. Secure HTTP (S/HTTP)

   Secure HTTP is an alternative approach to SSL, developed in 1993-94 (earlier than SSL). It was designed to be a security enhancement of the HTTP protocol and includes the following features:

   - authentication
   - encryption
   - cryptographic checksums
   - digital signatures

   Secure HTTP has greater functionality than SSL because it is integrated into the HTTP protocol, but users need to install a specific Web browser to use S/HTTP.

4. Secure Electronic Transaction (SET)

   Developed by two major credit card companies, SET provides a protocol and infrastructure specification that supports bank payments which can be integrated into any Web site. SET provides the following capabilities

   - encrypts payment instructions that precludes exposure of a user's credit card number (on the network and on the merchant's system)
   - authenticates merchants to users to protect against impostors

- optionally provides authentication of users to protect against unauthorized persons who attempt to initiate a bank payment

The technologies described above can be used to meet a range of security requirements. They can be deployed individually or in conjunction with one another.

The table below provides an indication of the requirements that can be satisfied by technology currently in use.

Technology/Requirement	Basic Authentication	SSL	SET
User Authentication	yes (cleartext passwords)	optional (certificates)	optional (certificates)
Server Authentication	No	yes (certificates)	yes (certificates)
Confidentiality	No	yes	yes (for credit card information)
Integrity	No	yes (with Server Authentication)	yes

In selecting authentication and encryption technologies, consider the following guidelines:

- Basic Authentication can be used to authenticate users. SSL encryption needs to be added to protect against sniffers and intruders posing as authorized users.
- SSL User Authentication provides a "stronger" solution than Basic Authentication. This technology provides a more secure and complete description of a user's attributes and it does not rely on users remembering their passwords. It does, however, require some form of PKI for verifying certificates and managing keys.
- Choose SET if only credit card information needs to be protected. The use of SET requires cooperation with the banking industry. SSL provides a much simpler solution if you only need to protect the transfer of credit card information against sniffers.
- To protect users against bogus Web sites (posing as a site that they are not), use SSL server authentication in conjunction with a SSL server certificate from a trusted CA.
- Use SSL to protect against network sniffers and the unauthorized alteration of Web content during transmission.

- Install and configure the Web server software to support the use of SSL if confidentiality is needed

- Create a SSL server key and the related certificate request. Arrange for a CA to provide a certificate for your public SSL server key

- Configure your Web server software to support the use of SSL and basic authentication if users need to be authenticated

- Configure your Web server software to support the use of SSL client certificates if stronger authentication is needed

- Configure the Web server to support the use of SSL or SET if credit card information needs to be transmitted

WEB SECURITY CHECKLISTS

[Extracted from NIST Special Publication 800-44 "Guidelines on Securing Public Servers"]

The following tables summarize, in the form of checklists, the steps that need to be taken by health data organizations to secure their Web sites, including both Web server security and Web site security

Part I: Web Server Security Checklist

Completed	Action
	Plan the configuration and deployment of Web server
☐	Identify functions of Web server
☐	Identify information categories that will be stored, processed and transmitted through the Web server
☐	Identify security requirements of information
☐	Identify how information is published to the Web server
☐	Identify a dedicated host to run Web server
☐	Identify network services that will be provided and supported by the Web server
☐	Identify users and categories of users of the Web server and determine privilege for each category of user
☐	Identify user authentication methods for Web server
	Choose appropriate operating system for Web server
☐	Minimal exposure to vulnerabilities
☐	Ability to restrict administrative or root level activities to authorized users only
☐	Ability to deny access to information on the server other than that intended to be available

Completed	Action
☐	Ability to disable unnecessary network services that may be built into the operating system or server software
☐	Ability to control access to various forms of executable programs, such as Computer Gateway Interface (CGI) scripts and server plugins in the case of Web servers
☐	Availability of experienced staff to install, configure, secure, and maintain operating system
	Patch and upgrade operating system
☐	Identify and install all necessary patches and upgrades to the operating system
☐	Identify and install all necessary patches and upgrades to applications and services included with the operating system
	Remove or disable unnecessary services and applications
☐	Disable or remove unnecessary services and applications
	Configure the operating system user authentication
☐	Remove or disable unneeded default accounts and groups
☐	Disable noninteractive accounts
☐	Create the user groups for the particular computer
☐	Create the user accounts for the particular computer
☐	Check the organization's password policy, and set account passwords appropriately (e.g., length, complexity)
☐	Configure computers to deny login after a small number of failed attempts
☐	Install and configure other security mechanisms to strengthen authentication
	Test the security of the operating system
☐	Test operating system after initial install to determine vulnerabilities
☐	Test operating system frequently to determine new vulnerabilities

Section II: Installing and Configuring the Web Server Securely

Completed	Action
	Securely installing the Web server
☐	Install the server software on a dedicated host
☐	Install minimal Internet services required
☐	Apply any patches or upgrades to correct for known vulnerabilities
☐	Create a dedicated physical disk or logical partition (separate from operating system and server application) for Web content
☐	Remove or disable all services installed by the Web server application but not required (e.g., gopher, FTP, and remote administration)

Completed	Action
☐	Remove all sample documents, scripts, and executable code
☐	Remove all vendor documentation from server
☐	Apply appropriate security template or hardening script to server
☐	Reconfigure HTTP service banner (and others as required) NOT to report Web server and operating system type and version
	Configuring Web server host operating system access controls
☐	Configured so that Web content files can be read but not written by Web service processes
☐	Configured so that Web service processes cannot write the directories where public Web content is stored
☐	Configured so that only processes authorized for Web server administration can write Web content files
☐	Configured so that Web application can write Web server log files, but log files cannot be read by the Web server application
☐	Configured so that temporary files created by Web server application are restricted to a specified and appropriately protected subdirectory
☐	Configured so that access to any temporary files created by Web server application is limited to the Web service process(es) that created these files
☐	Installed with Web content on a different hard drive or logical partition than the operating system and Web application
☐	Configured so that if uploads are allowed to the Web server, a limit is placed on the amount of hard drive space that is dedicated for this purpose
☐	Configured so that log files are stored in a location that is sized appropriately
	Configuring a secure Web content directory
☐	Dedicate a single hard drive or logical partition for Web content and establish related subdirectories exclusively for Web server content files, including graphics but excluding scripts and other programs
☐	Define a single directory exclusively for all external scripts or programs executed as part of Web server content (e.g., CGI, ASP)
☐	Disable the execution of scripts that are not exclusively under the control of administrative accounts. This action is accomplished by creating and controlling access to a separate directory intended to contain authorized scripts
☐	Create the user groups for the computer.
☐	Disable the use of hard or symbolic links (a.k.a., shortcuts for Windows).
☐	Define a complete Web content access matrix. Identify which folders and files within the Web server document are restricted and which are accessible (and by whom)
☐	Check the organization's password policy, and set account passwords appropriately (e.g., length, complexity)
☐	Use robots.txt file if appropriate

Completed	Action
	Using file integrity checkers
☐	Install a file integrity check to protect Web server configuration files, password files and Web content
☐	Update file integrity checksums whenever an upgrade or content changed occurs
☐	Store checksum on protected write once media
☐	Regularly compare checksums

Section III: Securing Web Content

Completed	Action
	Ensure that none of the following types of information are available on or via a public Web server
☐	Classified records
☐	Internal personnel rules and procedures
☐	Sensitive or proprietary information
☐	Personal information about an organization's personnel
☐	Telephone numbers, e-mail addresses, or general listings of staff unless necessary to fulfill organizational requirements
☐	Schedules of organizational principals or their exact location (whether on or off the premises)
☐	Information on the composition, preparation, or optimal use of hazardous materials or toxins
☐	Sensitive information relating to homeland security
☐	Investigative records
☐	Financial records (beyond those already publicly available)
☐	Organization's physical and information security procedures
☐	Information about organization's network and information system infrastructure
☐	Information that specifies or implies physical security vulnerabilities
☐	Plans, maps, diagrams, aerial photographs, and architectural plans of organizational building, properties, or installations
☐	Copyrighted material without the written permission of the owner
☐	Privacy or security policies that indicate the types of security measures in place to the degree that they may be useful to an attacker
	Establish an organizational-wide documented formal policy and process for approving public Web content that
☐	Identifies information that should be published on the Web
☐	Identifies target audience
☐	Identifies possible negative ramifications of publishing the information
☐	Identifies who should be responsible for creating, publishing, and maintaining this particular information
☐	Provides guidelines on styles and formats appropriate for Web publishing

Completed	Action
☐	Provides for appropriate review the information for sensitivity and distribution/release controls (including the sensitivity of the information in aggregate)
☐	Determines the appropriate access and security controls
☐	Provides guidance on the information contained within the source code of the Web content
	Web user privacy considerations
☐	Published privacy policy
☐	Prohibition the collection of personally identifying data without the explicit permission of the user
☐	Prohibition on the use of "persistent" cookies
☐	Use of session cookie, if used, is clearly identified in published privacy policy
	Client side active content security considerations
☐	Used only when absolutely required
☐	No actions taken without express permissions of user
☐	No use of high risk client side active content
☐	When possible alternatives are provided (e.g., plain text provided along with PDF)
	Server side active content security considerations
☐	Simple easy to understand code
☐	Limited or no reading or writing of files
☐	Limited or no interaction with other programs (e.g., sendmail)
☐	No requirement to run with suid privileges
☐	Use of explicit path names (i.e., does not rely on path variable)
☐	No directories have both write and execute permissions
☐	All executable files are placed in a dedicated folders
☐	SSIs are disabled or execute function is disabled
☐	All user input is validated
☐	Dynamically created pages do not create dangerous metacharacters
☐	Character set encoding should be explicitly set in each page
☐	User data should be scanned for byte sequences that mean special characters for the given encoding scheme
☐	Cookies should be examined for any special characters
☐	Encryption mechanism is used to encrypt passwords entered through scripts forms
☐	For Web applications that are restricted by username and password, none of the Web pages in the application should be accessible without going through the appropriate login process
☐	All sample scripts are removed
☐	No third-party scripts or executable code are used without verifying the source code

Section IV: Employing Web Authentication and Encryption Technologies

Completed	Action
	Web authentication and encryption technologies
☐	For Web resources that require minimal protection and for which there is a small, clearly defined audience, configure address-based authentication
☐	For Web resources that require additional protection but which for which there is a small, clearly defined audience, configure address-based authentication as a second line of defense
☐	For Web resources that require minimal protection but for which there is no clearly defined audience, configure basic or digest authentication (better)
☐	For Web resources that require protection from malicious bots (see Section 5.2.4), configure basic or digest authentication (better)
☐	For Web resources that require maximum protection, configure SSL/TLS
	Configuring SSL/TLS
☐	For configurations that require minimal authentication but require encryption, use self-signed certificate
☐	For configurations that require server authentication and encryption, use third-party issued certificate
☐	For configurations that require a medium level of client authentication, configure server to require username and password via SSL/TLS
☐	For configurations that require a high level of client authentication configure server to require client certificates via SSL/TLS
☐	Configure file integrity checker to monitor Web server certificate
☐	If only SSL /TLS is to be used on the Web server, ensure access via TCP port 80 is disabled
☐	If most traffic to the Web server will be via encrypted SSL/TLS, ensure that appropriate logging and detection mechanisms are employed on the Web server (because network monitoring is ineffective against encrypted SSL/TLS sessions)

Section V: Employing Network Infrastructure to Secure Web Servers

Completed	Action
	Network location
☐	The Web server is located in a DMZ or outsourced to an organization that appropriately protects the firewall
☐	The DMZ is not located on the third (or more) interface of the firewall
	Firewall configuration
☐	Web server is protected by a firewall

Completed	Action
☐	Web server if it faces a higher threat or if it is more vulnerable, is protected by an application layer firewall
☐	Firewall controls all traffic between the Internet and the Web server
☐	Firewall blocks all inbound traffic to the Web server except TCP ports 80 (HTTP) and/or 443 (HTTPS using SSL/TLS)
☐	Firewall blocks (in conjunction with IDS) IP addresses or subnets that the IDS reports are attacking the organizational network
☐	Firewall notifies the network or Web administrator of suspicious activity through an appropriate means
☐	Firewall provides content filtering
☐	Firewall configured to protect against of service attacks
☐	Firewall detects malformed or known attack URL requests
☐	Firewall logs critical events
☐	Firewall and firewall operating system patched to latest or most secure level
	Intrusion detection systems (IDS)
☐	Host-based IDS used for Web servers that operate primarily SSL/TLS
☐	IDS configured to monitor network traffic before any firewall or filter router (network-based)
☐	IDS configured to monitor traffic network traffic to and from the Web server after firewall
☐	IDS configured to monitor changes to critical files on Web server (host-based or file-integrity checker)
☐	IDS blocks (in conjunction with the firewall) IP addresses or subnets that are attacking the organizational network
☐	IDS notifies the network or Web administrator of attacks through appropriate means
☐	IDS configured to detect port scanning probes
☐	IDS configured to detect DoS
☐	IDS configured to detect malformed URL requests
☐	IDS configured to log events
☐	IDS updated with new attack signatures frequently (weekly basis)
☐	IDS configured to monitor the system resources available on the Web server host (host-based)
	Network switches and hubs
☐	Network switches are used on Web server network segment to protect against network eavesdropping
☐	Network switches are configured in high-security mode to defeat ARP spoofing and ARP poisoning attacks
☐	Network switches are configured to send all traffic on network segment to IDS host (network-based)

Section VI: Securely Administering a Web Server

Completed	Action
	Logging
☐	Use the Combined Log Format for storing the Transfer Log or manually configure the information described by the Combined Log Format to be the standard format for the Transfer Log
☐	Enable the Referrer Log or Agent Log if the Combined Log Format is unavailable
☐	Establish different log file names for different virtual Web sites that may be implemented as part of a single physical Web server
☐	Use the Remote User Identity as specified in RFC 1413
☐	Store logs on a separate (syslog) host
☐	Archive logs according to organizational requirements
☐	Review logs daily
☐	Review logs weekly (for more long-term trends)
☐	Use automated log file analysis tool(s)
	Web server backups
☐	Create a Web server backup policy
☐	Back up Web server incrementally on a daily to weekly basis
☐	Back up Web server fully on a weekly to monthly basis
☐	Periodically archive backups
☐	Maintain an authoritative copy of Web site(s)
	Recovering from a compromise
☐	Report incident to organization's computer incident response capability
☐	Consult the organization's security policy
☐	Isolate compromised system(s) or take steps to contain attack so additional evidences can be collected
☐	Investigate other "similar " hosts to determine if the attacker also has compromised other systems
☐	Consult, as appropriate, with management, legal counsel, and law enforcement officials expeditiously
☐	Analyze the intrusion
☐	Restore the system
☐	Reconnect system to network
☐	Test system to ensure security
☐	Monitor system and network for signs that the attacker is attempting to access the system or network again
☐	Document lessons learned
	Security testing
☐	Periodically conduct vulnerability scans on Web server and network supporting network
☐	Update vulnerability scanner prior to testing

Completed	Action
☐	Correct any deficiencies identified by the vulnerability scanner
	Remote administration and content updating
☐	Use a strong authentication mechanism (e.g., public/private key pair, two factor authentication)
☐	Restrict hosts that can be used to remotely administer or update content on the Web server by IP address and to the internal network
☐	Use secure protocols (e.g., secure shell, HTTPS)
☐	Enforce the concept of least privilege on the remote administration and content updating (i.e., attempt to minimize the access rights for the remote administration/update account[s])
☐	Change any default accounts or passwords from the remote administration utility or application
☐	Do not allow remote administration from the Internet through the firewall
☐	Do not mount any file shares on the internal network from the Web server or vice versa

Section VII: Securing Apache

Completed	Action
	Installing and securing the host operating system
☐	Apply latest patches to operating system
☐	Disable or remove all unnecessary services and applications
☐	Apply appropriate permissions to system resources
☐	Use appropriately strong identification and authentication mechanisms
	Installing the Apache Web server software
☐	Install Apache daemon and Web server content on separate hard drive partitions
☐	Web content should be stored in the DocumentRoot
☐	DocumentRoot and htdocs should be installed in separate directories
☐	Remove all Apache and other vendor documentation from DcoumentRoot and htdocs directories
☐	Install Apache in a chroot jail
☐	Do not install or remove src directory included in the Apache distribution
	Set permission for the Web server directories and files
☐	Ensure that all commands executed by root are protected from nonroot users
☐	Create an unprivileged user account for the Apache Web server
	Remove all unnecessary scripts, executables, and services
☐	Disable or remove unnecessary services and applications

Completed	Action
☐	Remove all sample content
☐	Remove all unnecessary scripts and executables (e.g., CGI, PHP, etc.)
☐	Delete all unnecessary files from the HTML document tree
☐	Prevent users from creating .htaccess files
	Initial configuration
☐	Make working copies of the server configuration files
☐	Disable automatic directory listing
☐	Disable symbolic links
☐	Disable server side includes
☐	Enable logging
☐	Configure user identification and authentication as appropriate
☐	Restrict remote operations put and post
	Maintaining a secure Apache configuration
☐	Apply all necessary patches to the Apache application (check for new patches on (at least) a weekly basis)
☐	Employ vulnerability scanners to test Apache install, underlying operating system and network defenses (when installed and at least quarterly thereafter)
☐	Monitor logs on a daily basis
☐	Archive and flush Web server logs periodically
☐	Perform regular backups of system data and Web server content

Section VIII: Securing Microsoft Internet Information Server

Completed	Action
☐	Implement SSL for all Web sites (where applicable)
☐	Enable logging (W3C extended format)
☐	Set proper log file ACLs
☐	Backup logs offline weekly if not daily
☐	Remove all IIS sample applications
☐	Remove unused script mappings
☐	Disable RDS Support
☐	Disable IPP Support (IIS 5.x only)
☐	Disable parent paths
☐	Enable strong authentication for protected resources
☐	Set NTFS directory permissions for Web folders
☐	Back up IIS Metabase frequently
☐	Run IIS Lockdown Tool

ATTACHMENT A
GLOSSARY OF TERMS

A

Accessibility

Congress enacted legislation (Section 508) that requires all web sites funded by Federal dollars to be accessible by those with physical handicaps. The World Wide Web Consortium (W3C) (**http://www.w3.org/**) has guidelines that explain how to make Web content accessible to the widest possible audience (people using different hardware such as PDA, laptops, etc. as well as people with disabilities). You may also use Bobby WorldWide (**http://www.cast.org/bobby/**) to help identify changes that can be made to your pages so that users with disabilities can more easily use them.

Address Resolution Protocol

A protocol used to obtain a node's physical address. A client station broadcasts an Address Resolution Protocol (ARP) request onto the network with the Internet Protocol (IP) address of the target node it wishes to communicate with, and the node with that address responds by sending back its physical address so that packets can be transmitted.

Authoring Tools

These are software tools that can help simplify the process of creating Web pages. For more information about the software, follow the links below:
Dreamweaver: (**http://www.macromedia.com/software/dreamweaver/**)
Homesite: (**http://www.macromedia.com/software/homesite/**)
NoteTab (**http://www.notetab.com/**)
A comprehensive list of tools is available at
http://builder.cnet.com/webbuilding/pages/Authoring/ProdTools/

C

Content Management System (CMS)

Software that enables one to add and/or manipulate content on a Web site. Typically, a CMS consists of two elements: the content management application (CMA) and the content delivery application (CDA). The CMA element allows the content manager or author, who may not know HTML, to manage the creation, modification, and removal of content from a Web

site without needing the expertise of a Webmaster. The CDA element uses and compiles that information to update the Web site. The features of a CMS system vary, but most include Web-based publishing, format management, revision control, and indexing, search, and retrieval.

Cookies

Cookies are a small piece of text information which an HTTP server can send to a browser to be stored. This same piece of information can then be transmitted back to the server from the browser when subsequent requests are made. The main use of cookies is to preserve "state" information, or information which can persist between requests to a server. An example of this use would be to send a unique identifier to a browser after a form is filled out. Subsequent requests for this form cause the unique identifier to be sent back. This allows the server to look up the original form information and use it.

Many users, especially those interested in medical conditions or sensitive subjects, may be reluctant to accept or return cookies to these web sites. web sites should be designed to function without error in the absence of cookies, even though this may require extra effort on the part of the user, to re-type information, for example:

Cookies that store or transmit information that falls under the HIPAA or FERPA Acts should do so from secure, encrypted servers.

More technical information on cookies can be found at:

Definitions and technical aspects:
http://www.ufaq.org/navcom/lyncookie.html
Privacy concerns: http://www.junkbusters.com/cookies.html
Web site devoted to cookies and privacy: http://cookiecentral.com/
Short page on cookies: http://isis.rte.ie/newradio/cookiedef.html

Copyright

By law, copyright exists from the time of creation of "an original work of authorship fixed in a tangible medium of expression." Today there is no need to put a copyright notice to have a copyright. Registration is not required to bring an action for infringement, but if the copyright was registered prior to the infringement, certain statutory damages are available which are not available if the copyright is not registered.

It is a matter of good practice to place a copyright notice which includes the copyright holder and year of creation. Changing items, which include

some new work and some work created in prior years can include the multiple years.

Colors

By combining foreground and background colors with sufficient contrast, visitors with color deficits will be able to see your pages more easily.

Counters

Access counters are small graphics, usually at the bottom of a page, that record the number of times the page has been requested from the server. Access counters are more suited for personal sites and do little to accurately record site visits.

D

Digital Millennium Copyright Act (DMCA)

The Digital Millennium Copyright Act, signed into law on October 28, 1998, amended the copyright law to provide limitations for service provider liability relating to material online. New subsection 512(c) of the copyright law provides limitations on service provider liability with respect to information residing, at direction of a user, on a system or network that the service provider controls or operates, if the service provider has designated an agent for notification of claimed infringement by providing contact information to the Copyright Office and through the service provider's publicly accessible website.

F

Font Families

Although many computers have the same basic fonts preinstalled, you cannot guarantee this. Hence, it is advisable to provide multiple fonts for the browser to choose from. If the first choice is not available, the browser will look for the second, third, etc.

Always include a generic font as the last choice. The generic font names are serif, sans-serif, cursive, monospace, and fantasy.

Here are some examples using the font tag:

<font face="Verdana, Arial, Helvetica, sans-serif">
<font face="Georgia, Times New Roman, serif">
<font face="Courier, monospace">

And here are the same examples using CSS:
font-family: Verdana Arial Helvetica sans-serif;
font-family: Georgia 'Times New Roman' serif;
font-family: Courier monospace;

For more information about fonts, see Webmonkey: Design: Fonts.

Font Size

It is preferable to keep font types relative rather than absolute, so that visitors can adjust the sizes in their browsers.

With the font tag, use <font size="-2"> or <font size="+1"> instead of <font size="1"> or <font size="4">. With CSS, use font-size: 80%; or font-size: larger; instead of font-size: 10pt; or font-size: 18px;

For more information about font sizes, see http://www.useit.com/alertbox/9707a.html.

Frames

There is much debate about frames. Read about the pros and cons of using frames, at **http://www.yourhtmlsource.com/frames/goodorbad.html**

G

Graphics

For usage check the Images section below.
For more information about software tools, follow the links below:
Fireworks: (**http://www.macromedia.com/software/fireworks/**)
Illustrator or Photoshop **(http://www.adobe.com/web/main.html**)
PaintShop Pro or WebDraw (**http://www.jasc.com/**)

H

Health Insurance Portability and Accountability Act (HIPAA) <JHU> (top)

The Health Insurance Portability and Accountability Act (HIPAA) has as one of its main purposes the simplification and efficiency of the transmission of health information. But this simplification and efficiency is not to be at the expense of the security and privacy of the health information. The Act itself presents a balanced approach to these various purposes. For more information select the HIPAA button at the top of this page.

Host

The term can refer to almost any kind of computer, from a centralized mainframe that is a host to its terminals, to a server that is host to its clients, to a desktop personal computer (PC) that is host to its peripherals. In network architectures, a client station (user's machine) is also considered a host because it is a source of information to the network in contrast to a device such as a router or switch that directs traffic.

Hoftfix

Microsoft's term for a bug fix, which is accomplished by replacing one or more existing files in the operating system or application with revised versions.

HTML Editors

Check Authoring tools above.

I

Identification/Contact Information

It is helpful for a site (and ideally every page within a particular site) to identify its Web developer and content provider. For an example, see the BSPH contact page: (**http://www.jhsph.edu/Contact/index.htm**)

Images

To keep page load time to a minimum, keep the size of a graphic (GIF and JPG) under 30 kilobytes and the total number of graphics on any page to a minimum. Including HEIGHT and WIDTH tags for all images helps them load faster.

Provide text equivalents for all non-text elements (e.g., images, image map regions, graphical representations of text, etc.) so that those who view your pages without images will be able to understand it.

For more information about formatting and optimizing for the web, see Webmonkey: Design: Graphics, or Web Reference: Optimizing Graphics.

J

Javascript

Since not all visitors have JavaScript or Java enabled on their systems, include the <noscript> code in a page that uses JavaScript so that visitors

will know that the page requires JavaScript. Keep in mind that JavaScript rollovers take longer to load and will add to overall page memory.

L

Language Attributes

To assist search engines, speech synthesizers, spell checkers, and grammar checkers, identify the primary natural language of a document by setting the "lang" attribute on the HTML element. See the W3C's guidelines More info: **http://www.w3.org/TR/html401/struct/dirlang.html#h-8.1**

Links

It is preferable to use document-relative links instead of root-relative links as this makes your site more portable. The rationale behind this is that root-relative links are interpreted by servers, not by browsers. Therefore, if you open a local page that uses root-relative links in your browser, the links won't work.

M

Mandatory Access Control

A means of restricting access to system resources based on the sensitivity (as represented by a label) of the information contained in the system resource and the formal authorization (i.e., clearance) of users to access information of such sensitivity.

Metadata

Adding metadata to your source code provides valuable information about the content of your web site. Some of their uses include identifying a page's creator, HTML specs, keywords, description, and refresh parameters. View the W3C's Metadata and Resource Description (**http://www.w3.org/Metadata/**) to learn more.

N

Navigation

It helps to have consistent navigation on every page of your site so that visitors will find their way around your site. It is also helpful to include a link to the home page from every page in your site so that you don't have "orphan" pages.

It is advisable to keep the amount of clicking to a minimum. Ideally, a site's home page has direct links to all of its sub-pages so visitors only need to click 2 or 3 times from the home page to get to any page within the site. If this is not the case, you may want to consider restructuring your web site.

Finally, keep the amount of scrolling required on each page to a minimum.

Network Administrator

A person who manages a local area network (LAN) within an organization. Responsibilities include network security, installing new applications, distributing software upgrades, monitoring daily activity, enforcing licensing agreements, developing a storage management program, and providing for routine backups.

Nonce

A Nonce is a randomly generated value used to defeat "playback" attacks in communication Protocols. One party randomly generates a nonce and sends it to the other party. The receiver encrypts it using the agreed upon secret key and returns it to the sender. Since the sender randomly generated the nonce, this defeats playback attacks because the replayer cannot know in advance the nonce the sender will generate. The receiver denies connections that do not have the correctly encrypted nonce.

O

Operating System

The master control program that runs the computer. The first program loaded when the computer is turned on, its main part, the "kernel," resides in memory at all times. The operating system sets the standards for all application programs that run in the computer. The applications "talk to" the operating system for all user interface and file management operations.

P

Page Layout

It is advisable to set table widths so that visitors with small screens do not need to scroll right to read your page. Images or groups of images should be sized appropriately for that reason as well. In addition it helps to keep

all or most of your information "above the fold" so that users do not have to scroll down excessively. To read more about page layout, visit http://www.wpdfd.com/editorial/wpd0601.htm.

Page Load Time

It is preferable to keep the size of an HTML file under 32 kilobytes. If a Web page exceeds this size, consider creating multiple pages in place of the single file. There are exceptions to this guideline, however, like when you have media-rich pages.

Patch

A patch (sometimes called a "fix") is a "repair job" for a piece of programming. A patch is the immediate solution that is provided to users; it can sometimes be downloaded from the software maker's Web site. The patch is not necessarily the best solution for the problem, and the product developers often find a better solution to provide when they package the product for its next release. A patch is usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a binary file or object module). In larger operating systems, a special program is provided to manage and track the installation of patches.

Plugins

If an element on your page requires a plugin (e.g., Adobe Acrobat, Flash, Shockwave, Realtime, Quicktime, etc.), provide information on where the plugin can be obtained. Consider placing plugin detects in your code.

Proxy

A proxy is an application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. This effectively closes the straight path between the internal and external networks. Making it more difficult for an attacker to obtain internal addresses and other details of the organization's internal network. Proxy servers are available for common Internet services; for example, an Hyper Text Transfer Protocol (HTTP) proxy used for Web access, and an Simple Mail Transfer Protocol (SMTP) proxy used for e-mail.

R

Resources and References

There are web development classes offered at Hopkins, and many resources available on the Web.

S

Section 508: Web Accessibility

Section 508 is an amendment to the Rehabilitation Act of 1973. Section 508 went into effect on June 21, 2001 and it requires that Federal agencies' electronic and information technology, including computers, software, and electronic office equipment, is accessible to people with disabilities, including employees and members of the public. Section 508 criteria spell out what makes these products accessible to people with disabilities, including those with vision, hearing, and mobility impairments.

Standards include technical criteria specific to various types of technologies and performance-based requirements, which focus on the functional capabilities of covered technologies. Specific criteria covered controls, keyboards, and keypads; software applications and operating systems (non-embedded); web-based information or applications; telecommunications functions; video or multi-media products; and information kiosks and transaction machines. Compatibility with adaptive equipment that people with disabilities commonly use for information and communication access is also covered.

Service Pack

A software patch that is applied to an installed application. It is either downloaded from the vendor's Web site or distributed via Compact Disc Read Only Memory (CD-ROM). When executed, it modifies the application in place.

Site Maps/Indexes

Site maps/indexes provide helpful information about the layout of a site and are another helpful navigation tool for visitors.

Statistics

There are many tools available for analysis of web site traffic. Logging needs to be enabled on your web server to record visits. These log files are then analyzed by software such as Webtrends or Analog and reports are generated. Analysis of web site traffic is not an exact science, and there are those who feel Web Usage Statistics Are (Worse Than) Meaningless (http://www.cranfield.ac.uk/docs/stats/). .

System Administrator

A person who manages a multi-user computer system and whose responsibilities are similar to that of a network administrator. A system

administrator would perform systems programmer activities with regard to the operating system and other network control programs.

T

Testing

It is advisable to test your web site on different versions of both Netscape and Explorer as well as the Windows and Macintosh platforms to make sure all pages function properly. You may also use a free tool like Xenu to check your web site for broken links.

V

Vulnerability

A security exposure in an operating system or other system software or application software component. A variety of organizations maintain publicly accessible databases of vulnerabilities based on the version number of the software. Each vulnerability can potentially compromise the system or network if exploited.

W

Web Administrator

The Web equivalent of a system administrator. Web administrators are system architects responsible for the overall design, implementation, and maintenance of a Web server. They may or may not be responsible for Web content, which is traditionally the purview of the Webmaster (see below).

Webmaster

A person responsible for the implementation of a Web site. Webmasters must be proficient in hypertext markup language (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, which is traditionally the responsibility of the Web administrator (see above).

Web Server

A computer that provides World Wide Web (WWW) services on the Internet. It includes the hardware, operating system, Web server software, Transport Control Protocol (TCP)/Internet Protocol (IP), and the 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."

ATTACHMENT B
RESOURCES

National Institute of Standards and Technology (NIST). Guidelines on Securing Public Web Servers. Special Publication 800-44. Washington, DC, September 2002.

[Note: This NIST Publication includes a comprehensive list of technical and non-technical resources for securing public web sites]

Department of Information Resources, State of Texas. World Wide Web Design Standards and Coding Guidelines. May, 2003
http://www.dir.state.tx.us/standards/srrpub11.htm

Department of Information Resources, State of Texas. World Wide Web Design Standards and Coding Guidelines - Transaction Risk Assessment. August, 2003
http://www.dir.state.tx.us/standards/srrpub11-transaction-risk.htm

The World Wide Web Security Frequently Asked Questions (FAQs) -
http://www.w3.org/Security/Faq/www-security-faq.html

Alliance for Electronic Business (AEB). Web Security Guidelines. Intellectuk, London, UK. 2002.

Allen, Julia, et al. Securing Network Servers (CMU/SEI-SIM-010). Pittsburgh, PA.: Software Engineering Institute, Carnegie Mellon University, 2000.

Allen, Julia & Stoner, Ed. Detecting Signs of Intrusion (CMU/SEI-SIM-009). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 2000.

Fithen, William, et al. Deploying Firewalls (CMU/SEI-SIM-008). Pittsburgh, PA.: Software Engineering Institute, Carnegie Mellon University, 1999.

Ford, Warwick & Baum, Michael. *Secure Electronic Commerce*. Prentice-Hall, 1997.

Garfinkel, Simon & Spafford, Gene. *Web Security & Commerce*. O'Reilly, 1997.

Kessler, Gary G. "Web of Worries." *Securing Your Web Site*. February 2000.

Kossakowski, Klaus-Peter, et al. Responding to Intrusions (CMU/SEI-SIM-006). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1999.

Larson, Eric & Stephens, Brian. *Web Servers, Security & Maintenance*. Prentice Hall, 2000.

Laurie, Ben & Laurie, Peter. *Apache – The Definitive Guide*. O'Reilly, 1997.

Rubin, Aviel; Geer, Daniel; & Ranum, Marcus. *Web Security Source book. John Wiley & Sons, 1997.*

Rubin, Aviel & Geer, Daniel. "A Survey of Web Security." *IEEE Computer*. September, 1998.

Soriano, Ray & Bahadur, Gary. "Securing Your Web Server." *Sys Admin*. May 1999.

Spainhour, Stephen & Quercia, Valerie. *Webmaster in a Nutshell*. O'Reilly, 1996.

Stein, Lincoln. *Web Security: A Step-by-Step Reference Guide*. Addison-Wesley, 1998.