Web Server Security Standard

Background

The University of Cincinnati data network is a shared resource used by the entire university community and its affiliates in support of the university's business practices and academic missions. Access to the data network is both an essential tool for university life and work and a valuable privilege. University units and community members must cooperate to protect the network by securing computer and network devices in order to preserve that access.

The Chief Information Officer (CIO) is responsible for the efficient, effective and secure operation of the university data network. Concurrently, academic, administrative and support units are responsible for the efficient, effective and secure operation of their local networks.

The Web Server Security Standard (WSSS) establishes security requirements for web servers, web applications, and web services that are critical to the University of Cincinnati. The standard is intended to help protect the university's central and distributed telecommunications and computing environment from accidental or intentional damage. The standard is also intended to protect the university's connected assets from alteration or theft of data while preserving university community members' appropriate access and use.

The WSSS is one of the interrelated IT Security Policy supporting standards, each of which addresses a different aspect of computer, network and data security. These include the Client Computer Security Standard, Critical Server Security Standard, Database Computer Security Standard.

This standard applies to servers that host web servers, web services or web applications and that have been deemed 'critical' based on the criteria in the Critical Server Security Standard section of the UC Critical Server Security Standards - whether owned by the university, a university community member or a 3rd party organization - that connect to the university data network or support infrastructure either directly or indirectly.

This standard outlines the responsibility of all university community members, including students, faculty, staff, agents, guests, or employees of affiliated entities. This includes (a) individuals who connect a device, either directly or indirectly, to the university data

network or support infrastructure, (b) individuals who install, maintain, or support a critical server, (c) individuals who develop, deploy, or maintain an application that resides or runs on a critical server, and (d) individuals who maintain or support a web server, or anyone who develops, deploys, or maintains a web application or other web content.

The Web Server Security Standard

The server hosting the web server, web service, or web application must comply with the UC Client Computer Security Standard and the UC Critical Server Security Standard.

All servers that host web servers, web services, or web applications and that have been deemed 'critical' based on the criteria in Critical Server Security Standard section of the UC Critical Server Security Standards must comply with this standard. A portion of those criteria are repeated here for the reader's convenience:

A 'critical' computer meets at least one of the following criteria:

1. It contains or serves Restricted Data, as defined in the Data Governance & Classification Policy Loss of service carries a significant financial liability, including grants and contracts.
2. Loss of service results in a significant negative impact(s) for the unit or for the reputation of the university.
3. Unit administration deems the server to be critical.

Installation and Configuration

Since often web servers exist as applications on a host operating system, they require special considerations during the configuration and installation phase of deployment

Technical staff MUST:

1. Configure web services in accordance with vendor security recommendations.
2. Ensure that only those web services or applications specifically needed should be enabled. Web services, applications, and sample content which is not needed should be disabled.
3. Patch web server software and web applications to all current security patches, as required by the UC Critical Server Security Standard. Software developed by vendors or developers unresponsive to patching security vulnerabilities should be replaced with alternative software. If alternative software is not available, a responsible party may assume patching responsibility, or compensating controls must be put into place.
4. Configure the web server to allow access only to data that is meant to be publicly available. Configure a robots.txt file to properly protect content from automatic

collection by web crawlers. "Obscure" or "secret" file or directory names must NOT be used to protect content.
5. Monitor comments on blogs and other forums if anonymous posting is allowed. This responsibility may be delegated to non-technical staff as deemed appropriate by the department or unit.
6. Prohibit web servers and web applications to run with elevated privileges (e.g. “root” or “Administrator”).
7. Use secure mechanisms to allow developers to install new or update existing content. Traditional FTP or other unencrypted password-based systems must not be used. Alternative protocols that provide encryption and secure authentication (e.g. SSH/SCP, SFTP, and rsync/SSH) must be used.

Technical staff SHOULD:

1. Store content uploaded through web applications outside of the document root.
2. Limit the ability of web server and web application user accounts to modify other programs, logs, or system configuration files by limiting account privileges.

Logs

Technical staff MUST:

1. Develop or configure web servers and applications to write logs that are adequate for incident response and security investigations. Useful log information includes, but is not limited to: Failed and successful login attempts, Account privilege changes and Timestamp information. Logs must contain the URLs as requested by the client. Logs must be retained for a minimum of 90 days, as with Critical Server Security Standard.
2. Keep discrete log files for each virtual web server If there are multiple virtual web servers hosted on a single server instance.
3. Copy web service logs to a separate secure log server for retention.

Encryption

Technical staff MUST:

1. Encrypt all Restricted Data (as defined by the Data Governance & Classification Policy).
2. Use commercially signed or authorized certificates for web services outside of the department or unit.
3. Renew certificates before their expiration date.

Secure Software Design, Implementation, and Testing Procedures

Unit administrative staff SHOULD:

1. Train those who develop web applications in secure code design, implementation, and testing procedures.
2. Review code to identify and correct common mistakes where possible or appropriate before deployment.

Technical staff SHOULD:

1. Prevent the error messages from underlying systems and processes from being publicly available to the web browser.
2. Only use active client-side and server-side content when absolutely necessary, and then with extreme caution.
3. Frequently and regularly scan web services for vulnerabilities (e.g. SQL injection flaws, cross-site scripting).

Compliance

Standards Compliance

All designated critical devices must comply with the UC Critical Server Security Standard.

In some cases it may not be possible to bring a device into compliance. For example, older laboratory equipment software may not operate with current operating systems or security patches. In these cases operating units or individuals and their information technology staff must employ compensating controls. In rare cases an exception may be made if no compensating control is possible.

Units must internally document requested compensating controls and any exceptions. These must be reviewed, tested, and approved by the UCIT Office of Information Security and the operating unit or individual must retain the approved documentation for audit so long as the device is in operation.

Registration of Critical Servers

Units are required to register all critical servers. Technical staff must register all IP addresses and DNS host names and 24/7 contact information for the administrators who are responsible for the servers. Information identifying department or controlling unit is also required.

Role of Units, IT staff, and others

The user's department/unit is responsible for ensuring compliance with the CCSS, though departmental/organization IT staff may perform the actual implementation on university owned equipment.

The user is responsible for compliance on personally owned equipment. Users granted responsibility for administration on university equipment will share responsibility for compliance with local IT staff. (i.e. local administrator rights, users granted access via a local administrative privilege standard policy)

Individual university community members who do not comply with this standard are in violation of the policy on the Acceptable Use of University Information Technology Resources and the Data Governance & Classification Policy. In accordance with that policy, violators may be denied access to university computing resources and may be subject to other penalties and disciplinary action including university disciplinary procedures.

Units are required to register all critical servers. Technical staff must register all IP addresses and DNS host names and 24/7 contact information for the administrators who are responsible for the servers. Information identifying department or controlling unit is also required. Units are expected to maintain local records of critical servers as well.

Role of UCIT Information Security

IT@UC Office of Information Security is tasked with the responsibility of maintaining the CCSS standard and ensuring that the document is kept current with threats and technologies going forward. IT@UC Office of Information Security will include community feedback and do publicity for any changes to the document.

IT@UC Office of Information Security members are also identified as the enterprise subject matter experts on information security practice and policy and in that role can be asked to perform security assessments or consultations with university units.

Compliance Mechanisms

Compliance with the standard can be accomplished using a variety of technological or practical tools. Units that have the capability to perform automated detection of patches and vulnerabilities (such as Altiris, LANdesk, Cisco Clean Access, Juniper NAC, etc.) should use these tools to do regular inspection of their networks to gather information regarding the state of compliance.

Those units that do not have the capability to run automated tools to gather compliance information are encouraged to consider purchasing/acquiring these tools but may elect to use a manual process such as spot inspection of computers to determine overall compliance.

Units must conduct a compliance inventory on all university- managed devices on no less than a quarterly basis.

UCIT Information Security may conduct an inspection of unit resources in cooperation with the unit leadership and IT staff to determine overall CCSS compliance. These spot inspections are required if a unit is confirmed through investigation to have been involved in a CCSS related data breach.

Devices found not to be in compliance must be quarantined from the general network and the compliance issue must be addressed before it may be restored to normal operation. If the device cannot be made compliant the unit may implement a compensating control or request an exception. Upon approval of the exception request the device may be restored to normal operation.

Compliance Reporting

Units are expected to report to the Office of the Chief Information Officer on the details of CCSS compliance. Registered critical server information will be validated and maintained in a current status. Units are required to certify the accuracy of these registrations on a quarterly basis.

This information will be used for audit and compliance checking by OIS during required and random checks. These numbers are also reported up to the Board of Trustees. Units are encouraged to add comments when special circumstances surrounding compliance with the CCSS are identified. These comments will also help the university identify areas where compliance concerns exist and discussion of general technology solutions or security advice can be offered.

Designated members of each unit should file reports though colleges and larger departments may be asked to roll up report numbers to simplify the process of analysis. One administrative designee as well as at least one IT professional should be assigned the task of collecting and reporting this information.

Definitions

- **Anti-malware** – software designed to combat malware software by protecting computers from attack, neutralization or removal of the offensive programs.
- **Compensating controls** – a method of addressing the risk associated with a standard requirement by using alternative techniques to mitigate the risk.
- **Computer** - a desktop or mobile device (including smart phones, PDA, etc.) that is used primarily for normal desktop application work. With regards to the CCSS computer does not include computing devices with a dedicated use like building control systems or dedicated appliances that perform only a dedicated function. *This definition does not exclude desktop systems traditionally used for desktop purposes that are re-tasked for use in non-traditional roles. (i.e. lab instrument control)*

- **Data network** – a group of interconnected computers managed by The Ohio State University
- **Device** – for the purposes of this standard, device is an interchangeable term with the above definition of computer.
- **Data Trustee** – university administrators at the vice presidential level who bear the ultimate responsibility for ensuring the protection of the data stored by those in their reporting area
- **Data Steward** – university employees who have direct operational-level responsibility for information management
- **Data Custodian** – computer system administrators responsible for the operation and management of systems and servers which store or provide access to institutional data
- **Data User** – a university unit or community member using institutional data in the conduct of university business
- **Firewall software** – a part of a data network that is designed to block unauthorized access while permitting authorized communication. Firewalls can be software or dedicated computers that are configured to control computer traffic between different computer networks based upon a set of rules and other criteria.
- **Manually** – updated through a manual process, this process can include some automated tools but is generally accomplished using manpower resources and monitored directly by employees.
- **Non-compliant** – a device that does not meet the requirements of the standard.
- **Operating system** - The most important program that runs on a computer. Every general-purpose computer must have an operating system to run other programs.
- **UCNet** – the University of Cincinnati data network.
- **Password** - a sequence of characters that one must input to gain access to a file, application, or computer system.
- **Quarantine** – to isolate the device from other connected devices in a way that protects the device from exposure and prevents the device from potentially affecting the other resources on the data network.
- **Supported** – software and hardware that is currently receiving security updates by the manufacturer.
- **University-managed devices** – devices purchased, owned, gifted, granted and maintained by university employees. University-owned devices can include supported computer systems and devices purchased through any of the various funding models including but not limited to grants, endowment, direct purchase, etc.
- **User name** – a specific log in identity keyed to an individual user. User names are typically used to gain access to a computer operating system or application.
- **Viruses, spyware or adware** – a group of computer programs classified as “bad” or malware. Viruses, spyware and adware often exploit flaws in computer programs and operating systems to extract information or attack the integrity of a data network.

- **Web browser** - a computer program used for accessing sites or information on a network (such as the World Wide Web).

Tools:

Web Server Security Evaluation Checklist (**See Appendix A**)
Frequently Asked Questions **(See Appendix B)**

Related links:
Data Governance & Classification Policy
Vulnerable Systems Policy
Acceptable Use of University Information Technology Resources
Asset Disposition Policy

Contact Information
IT@UC Office of Information Security 513-558-ISEC (4732) Email: infosec@uc.edu

History:
Issued: 01/10/2013
Revised: 03/16/2017

Appendix A

Web Server Security Evaluation Checklist

A 'critical' computer meets at least one of the following criteria:
1. It serves restricted data, as defined in the Data Governance & Classification Policy.
2. Loss of service carries a significant financial liability, including grants and contracts.
3. Loss of service results in a significant negative impact(s) for the unit or for the reputation of the university.
4. Unit administration deems the server to be critical.

Statement	Must or Should?	Met	Not Met	Comments
Complies with UC Client Computer Security Standard	Must			
Complies with UC Critical Server Security Standard	Must			
a. Installation & Configuration				
Configure web services according to vendor security recommendations	Must			
Configure server to use ONLY needed web services or applications	Must			
Install all required updates and security patches prior to deployment of web server.	Must			
Configure server to only display public data.	Must			
Configure "robots.txt" or similar files to protect content.	Must			
Configure Moderation or assign personnel to monitor any blog or forum content if anonymous posting is allowed.	Must			
Prevent web servers or web applications from executing with "elevated" or admin privileges.	Must			
Use secure mechanisms to allow developers to install new or update existing content. Do not use traditional FTP or other unencrypted password-based systems.	Must			
Store all uploaded web content outside of document root.	Should			
Configure web services and web applications to use limited named accounts when modifying other programs, logs or configuration files.	Should			
b. Logging				
Configure web servers or applications to write logs containing login attempts (successful or failed), account modification (privilege changes, promotion, creation, deletion), timestamp, client access URLs.	Must			
Configure log retention of 90 days and plan for adequate storage space.	Must			
Create discrete logs for each server instance.	Must			
Copy web server/application logs to another log management server or location.	Must			
c. Encryption				
Configure web server/application to use SSL/TLS encryption to transfer/display restricted data.	Must			
Obtain a signed or authorized commercial certificate for web services accessed outside of the department/unit.	Must			
Renew certificates prior to expiration	Must			
d. Secure Software Design, Implementation, and Testing				
Ensure all web developers follow secure code design, implementation, and testing procedures.	Should			
Review code prior to updates/integration for coding errors and common mistakes.	Should			

Prevent error messages from publicly displaying information about underlying systems/processes or software.	Should			
Only use active client-side and server-side content when absolutely necessary, and then with extreme caution.	Should			
Scan web services for vulnerabilities.	Should			
Scan web applications for vulnerabilities	Must			

Appendix B

Web Service Security Standard (WSSS) Frequently Asked Questions

If I make a web service or server inaccessible outside of my department or unit, does this standard apply?

No, this standard applies only to servers that are accessible outside of a department or unit. However, all of the requirements of this document are strongly recommended for all web servers.

What is secure code?

Secure code is code that does not contain security vulnerabilities such as SQL injection flaws, Cross-Site Scripting vulnerabilities, etc.

What is a self-signed certificate versus a root certificate authority (CA)?

A self-signed certificate is it's own root CA. A self-signed certificate can not be validated because it is not signed by a well-known certificate root CA, therefore a client cannot be sure of the true identity of the server providing the self-signed certificate.

Why must I monitor anonymous comments?

Anonymous comments may be used to post inappropriate content, from which a severe loss of reputation to the University might ensue; or from which significant legal costs might be incurred.

Why should web uploads be stored outside of the document root?

The intent of this stipulation is to prevent someone from directly accessing content that they may have just uploaded. If someone uploads a PHP script to your web server, and your server is configured to store uploads within the main web site directory structure, and your server is configured to execute PHP scripts from within the main web site directory or sub-directories, then the uploader could directly request the URL to the uploaded file and have your server execute their script.

If you are unable to store uploads outside of your document root, there are a variety of ways to still permit uploads while protecting your site:

- Configure your server to not execute dynamic content (PHP, ASP, etc) from the directory in which you store uploads
- Configure your server to not permit direct requests to files stored in your upload directory

What are some resource for learning about and preventing SQL injections?

One of the most important assumptions about SQL injection is: assume that all data coming from the client (web browser) is suspicious. Preventing SQL injection then deals with filtering this data on the server side. If your scripting language allows parameterized queries, that is a great line of defense. For common scripting languages, here are some particular resources:

Functions for Storing Data Submitted From a Form

More generic information regarding SQL injections can be found at the following:

SQL Injection
SQL Injection Attacks by Example

What are some resources for learning about and preventing cross-site scripting vulnerabilities?

Generic information regarding Cross-Site Scripting can be found at the following:

Cross-Site Scripting
Cross-Site Scripting Flaw
Cross-Site Scripting Info
Preventing Cross-site Scripting Attacks

What logs would be useful for an incident investigation?

At the least, the web server's access and error logs are required. These permit the security response team to see what URLs were requested at what time by whom, as well as any error conditions that were reported as a result of these requests. Many attackers evaluate your server's response to invalid requests in order to learn of mistakes or vulnerabilities in your configuration.

If your web application records log data, that is useful. Any record of user logon (successes and failures), permission escalation (becoming an admin user in your web application, for example), or user activity (user "scott" modified the content of item #23 in the inventory system, for example) will help the security team.

What is server-side validation?

Server-side validation means that the web service residing on the web server hosting the web service validates the data input from a user before taking any action on it (e.g. inserting it into a database). This is in contrast to client-side validation, which is typically implemented using Javascript to validate the data with the user's browser before submitting it to the web service.

Does a proxy/security proxy server bring me into compliance?

No, a proxy server or proxy server providing security services (i.e. ISA Server) does not bring a server into compliance. However, any opportunity to implement layered security is recommended.