Web Security Standards

Author: Office of Information Technology (OIT)
Version 1.0
Last updated Aug. 14, 2015

Authority:
Duke University Chief Information Officer
Duke University Chief Information Security Officer

Introduction

Due to Duke’s broad web presence and the popularity of attacks against web servers, the security offices, in conjunction with campus IT and web development groups, have developed a set of web security standards intended to provide website owners/maintainers with guidance on securing websites in order to protect the sites from attacks.

Scope

These standards apply to Duke websites and web applications maintained on the Duke network or with a third party (external) hosting provider and to internal or third-party developers responsible for building or maintaining the websites.

Audience: (1) website/application owners, including their content editors and users, and (2) web service providers (website developers, web hosting providers).

Standards

The standards cover website and web application security, technical standards for implementing websites and applications, and web infrastructure management.

Web servers often have multiple administrators responsible for managing the different layers, from the operating system to the web server to the content management system (CMS). The following standards have been organized into five broad areas, with each section containing information about the general requirements that would apply across any technology used in the category. More detailed technical guidelines about specific technologies in use at Duke is available in an online wiki.

Server Configuration .................................................................2
HTTP Server Security ...............................................................2
Application Environment Security .................................................3
Server Configuration

All web and database servers should be hardened according to the ITSO Server Standard and configured to meet recommended system and vendor best practices. Specific requirements related to web servers are listed below. Additional Duke Medicine standards are available online at https://egrc.duhs.duke.edu/foundation/Workspace.aspx?workspaceId=-1&requestUrl.

1. Employ Shibboleth and multi-factor authentication (as needed) for user authentication and authorization whenever possible.
2. Only allow authentication to occur over an encrypted mechanism.
3. Patch and apply upgrades to the operating system on an ongoing basis (every two weeks at a minimum). Maintain up-to-date security fixes and patches (in accordance with Duke’s Vulnerability Management Policy). When applying security fixes and patches, the process should always include post-installation validation testing, either manual and/or using automated scanners.
4. Separate web server content and related subdirectories from operating system and application directories.
5. Enable only necessary services and applications; disable all others. This should extend to all add-ons, plugins, or tools that often accompany a default installation.
6. Create user accounts following the principle of least privilege providing only the level of access needed. Only use administrative accounts to perform administrator actions. Where/when possible, avoid using local accounts for administration because local accounts are more difficult to manage on a large scale.
7. Set all account passwords and change any default passwords (as installed by application software) to meet Duke password guidelines. If an application requires a password (e.g. service account), it should be complex and different for each application that needs one.
8. Review accounts, roles and permissions on a regular basis or whenever roles and users change.
9. Remove or disable unneeded default accounts.
10. Close all unnecessary firewall ports.
11. Turn on logging so that logs are available in the event they are needed for a security incident or operational issue. Review logs daily for unusual activity.
12. Perform daily backups of the operating system. Test the usability of backups at reasonable intervals to ensure the server can be recovered, if needed.
13. Check with the security office (security@duke.edu) to enroll server in a regular vulnerability scanning/testing schedule.

HTTP Server Security

Variations of HTTP servers include Apache, IIS, nginx, squid, and others. These applications must adhere to the following standards.
1. Patch and apply upgrades to your HTTP server on a routine basis (every two weeks at a minimum). Maintain up-to-date security fixes and patches in accordance with Duke’s Vulnerability Management Policy. When applying security fixes and patches, the process should always include post-installation validation testing, either manual or using automated scanners.

2. Run the webserver software as an unprivileged user and group, rather than as root or administrator. The user and group should not be used by other software and should not have more access to the file system than needed.

3. Disable unnecessary modules (such as WebDAV).

4. Turn on logging so that logs are available in the event they are needed for a security incident or operational issue. Review logs daily for unusual activity.

5. Perform daily backups of the web server. Test the usability of backups at reasonable intervals to ensure the server can be recovered, if needed.

**Application Environment Security**

Variations of application environments include PHP, Python, Perl, Java, JSP and others. Application environments in use on web servers must adhere to the following standards.

1. Patch and apply upgrades to your application environment on a regular basis (within two weeks of the release of a security fix) maintaining up-to-date security fixes and patches in accordance with Duke’s Vulnerability Management Policy.

2. Make sure that application environment does not run as the root user.

3. Set your application environment to log all errors in the event logs are needed for a security incident or operational issue.

**Database Security**

Variations of databases include MySQL, PostgresSQL, MongoDB, redis and others. Databases in use with web servers must adhere to the following standards.

1. Patch and apply database upgrades on a routine basis (within two weeks of the release of a security fix), maintaining up-to-date security fixes and patches in accordance with Duke’s Vulnerability Management Policy.

2. Restrict database access to specific hosts and users, only opening firewall ports to specific hosts.

3. Set passwords for any database users, and change any default passwords.

4. Change the database server default administrator username from the default name and set a strong password.

5. Run the database as a user other than root or administrator.

6. Enable logging. Always log errors, and set permissions so that only "root" and the database user account have access to the database error logs.

**CMS Security**

Variations of CMSs include Drupal, WordPress, Joomla, Wikis and others. CMS applications running on Duke web servers must adhere to the following standards. Additional requirements and best practices for specific technologies can be found online.
1. Patch and apply CMS core and module updates on an ongoing basis (within two weeks of the release of a security fix), maintaining up-to-date security fixes and patches in accordance with Duke’s Vulnerability Management Policy.
2. Rename the administrator account and make sure it is the only non-Shibboleth provisioned account on the site. Use Shibboleth for all other authentication.
3. Restrict CMS administration access to SSL only.
4. Turn on logging in the event logs are needed for a security incident or operational issue.

**Review Frequency:** Annually  
**Updated:** 14-Aug-15