Security Standard: Web

Scope

This standard applies to all web servers, services and applications (RIT and 3rd party) using web-oriented protocols.

The standard excludes embedded web servers that are not within the scope of the server standard, e.g., printers and other hardware devices.

Student web sites, services, and applications are subject to this standard if they are on the RIT web environment and publicly accessible.

Requirements

The following security controls are required to be implemented.

1. **Compliance with Other Standards**
   - 1.1. All servers within the scope of this standard should comply with the requirements of the Server Security Standard in addition to other relevant information security standards.
   - 1.2. Upon adoption, this standard shall become the security requirements that shall be incorporated into the RIT Web Standard.

2. **Registration**
   - 2.1. The department, owner, developer, administrator, and host location of web servers and services should be registered and updated as changes occur, and annually in the centralized registration system. The identified owner, developer, and administrator should be an RIT employee.

3. **Private Information Management**
   - 3.1. Private information should not be stored on web servers unless there is a legitimate business purpose approved by the Divisional VP and a security review has been conducted.

4. **Vulnerability Scanning & Penetration Testing**
   - 4.1. ITS will conduct vulnerability scans and penetration tests on a regular recurring basis
   - 4.2. Critical and severe vulnerabilities (as defined in the Server Standard) should be logged in a ticketing system or email and should be remediated, have a false positive reported, or have an exception filed within 1 month.
   - 4.3. Moderate vulnerabilities should be logged in a ticketing system or email and should be remediated, have a false positive reported, or have an exception filed within 1 month.

5. **Threat Management**
   - 5.1. Web system administrators are responsible for determining whether to implement a web firewall and/or a web application firewall or IPS. Recommended rule sets are available from the Information Security Office wiki.

6. Patching

6.1. Web servers, services, and applications should be patched within 5 business days after critical security patches are made available. Other non-critical patches should be evaluated and implemented based on the professional judgment of the server or application administrator.

6.2. Unpatched servers, services, and applications lacking critical security patches will be quarantined at the discretion of the CIO or Information Security Office.

6.3. Services and applications that no longer have vendor- or developer-provided security patches should be remediated or removed.

7. Minimum Encryption Levels

7.1. Web services should use, as a minimum, SSL version 3/TLS. Web services and applications should follow encryption best practices listed on the Information Security web site.

8. Content Filtering

8.1. Web applications should filter client input on the server following practices listed on the Information Security web site (http://www.rit.edu/security/content/client-input-filtering-practices).

8.2. The use of world-writeable files in web services and applications should be minimized to follow the practice of least privilege.

8.3. Application owners are responsible for monitoring the content on their website. Form spam is prohibited and should be removed immediately.

9. Logging (not applicable to student websites)

9.1. Web application logging should meet the requirements of the server/application standard.

10. Access controls

10.1. Root, service account, and administrator /user accounts should be different. The passwords for each account should be unique. The accounts should be used exclusively for the purpose for which they were created.

- 10.1.1. Web server-associated processes should run only under their own unique account. These accounts should not have root or administrator privileges.
- 10.1.2. All accounts should be authorized to provide the minimal level of access required

10.2. Stateless User Authentication

- 10.2.1. Session IDs should not be transmitted in clear text.

10.3. Web Services/Application Administrator Access Control

- 10.3.1. Configuration file write access should be limited to a web services/application administrative group.

10.4. Local Configuration File Use and Access Control

- 10.4.1. In order to prevent users from modifying the server configuration, Web Service/Application Administrators should limit access to user-modifiable configuration commands (e.g., .htaccess) according to a documented plan.

10.4.2. Web Service/Application Administrators should provide appropriate access controls for local configuration files.

11. Development & Acquisition (not applicable to student websites)

11.1. Web server, service, and application development or acquisition should meet the following requirements:

11.1.1. Follow documented development guidelines incorporating security or documented review process including security best practices available on the Information Security website.

11.1.2. Follow a documented sustainable maintenance program including security

11.1.3. Be executed by individuals with the training/education commensurate with their role.

12. Risk of Harm

12.1. The CIO, ISO, or their designees have the authority to take any website offline that poses a risk of harm to the RIT web environment.

12.2. The Service Desk will manage the communication and implementation of de-provisioning and re-provisioning websites.

Effective Date: January 23, 2015

Standard History:
May 15, 2008
September 15, 2011
November 11, 2013
October 19, 2015

Summary of Changes—Web Standard, 10/19/2015

We've made changes to the standard to incorporate the move of certain operational responsibilities from the ISO to ITS.

Section 4 changes

- Change responsibility of conducting vulnerability scans and pen tests on a regular recurring basis from ISO to ITS