CAL POLY POMONA
Web Application Code Development Standard
Developed in consultation with the
Information Security Governance Council
Al Arboleda, Dr. Debra Brum, Glendy Yeh, Kevin Morningstar, Lisa Rotunni, Mauricio Calderon,
Randall Townsend

Final: 4/30/09
Last Revised:
Web Application Code Development Standards

Purpose and Scope
The purpose of this standard is to increase the security of web applications and help safeguard university information technology resources. This standard applies to all web applications that are being developed or administered by the university staff, faculty, or auxiliary organizations.

Compliance with these requirements does not imply a completely secure application but these practices should be integrated into a comprehensive web application development plan.

Audience
All faculty, staff, student employees, contractors, and vendors developing or administering web applications designed to handle or manage university data.

Definitions

Web Application: A web application possesses all of the following observable properties:

- Web browser – Web applications use a web browser (technically a user agent) as a client. An application that uses the https protocol over the Internet to exchange information with a user, but uses a client that is not a web browser, is not a web application. WebDAV is an example of this.

- One-to-one relationship – Web applications establish a unique session and relationship with each and every visitor. This behavior is fundamental to Web applications and is not present in either content-based websites or desktop applications. A web application such as Yahoo mail knows who you are in a way that CNN or even Photoshop doesn’t.

- Ability to permanently change data – Web applications allow users to create, manipulate, and permanently store data. Such data can take the form of completed sales transactions, human resources records, or email messages to name but a few. This contrasts with web services like Google that allow users to submit information but do not allow them to permanently store or alter information.

Although these three characteristics alone result in a fairly broad definition of web applications, websites that possess all of them necessarily contain a degree of application behavior, logic, and state lacking in traditional content-based web sites. Websites that combine both content AND functionality should be considered web applications because they meet these criteria and therefore exhibit the interactive complexities and behaviors associated with applications.

The Open Web Application Security Project (OWASP) Top Ten: The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list. The U.S. Federal Trade Commission strongly recommends that all companies use the OWASP Top Ten to help locate potential security flaws. The Payment Card Industry (PCI) standard also recommends referencing the OWASP Top Ten.
**Protected Data:** Information that has been classified as Protected Information Levels 1 and 2 in the Campus Information Classification and Handling Standard. Please see that standard for more examples, but information so classified includes:

Personal Information (e.g., Passwords, SSN, birth date, drivers license)
- Financial Information (e.g., credit card, debit card, and bank account numbers)
- Health information
- Nonpublic student data
- Nonpublic employee data
- Other legally protected, contractually protected or nonpublic data

**Roles and Responsibilities**
This section identifies the roles and responsibilities for implementation and compliance of the standard.

- **Information Security Office Personnel (ISO)**— The ISO will complete or provide assistance to developers in the completion of security reviews.
- **Application Developers** – Campus staff and faculty software developers will comply with the web application code development standard.
- **I&IT Web Application Development Personnel** - I&IT Web Application Development personnel will review or provide assistance in the review of web application code for compliance with the university World Wide Web Policy and accessibility requirements.
- **Division IT Management** – IT management in each division will establish the expectation that the web application development procedures are documented and the standard is followed.

**Minimum Standard:**
This section lists the minimum standards that should be applied to the development and administration of web applications.

If a solution is not available for a specific requirement, then an alternate plan for risk management must be established. Data custodians, lead researchers, system administrators, and application developers are expected to use their professional judgment in managing risks to the information, systems and applications they use and/or support. All security controls should be proportional to the confidentiality, integrity, and availability requirements of the data processed by the system.

**Application source code must be protected from unauthorized access and tracked for version control**
Each campus division is responsible for defining its own change management processes that cover the management of application source code. When an application handles protected data, application developers must use version control management software that employs identity-based access controls for all source code, tracks versions, compares versions, and produces an examinable change log. I&IT has obtained version control management software that meets these requirements and has made it available for use by the campus community. Use of this software is recommended for all applications. In cases where dedicated version control software is not in use, change management processes should be employed to save, track and retrieve progressive versions of the application code, and allow for comparison of changes in current and previous versions. To allow for business continuity, source code in repositories should never be encrypted using individual keys.
Applications must be designed and tested for correct function and resistance to security exploits

Application developers must determine by both design and testing that each application:

1. Performs as specified by its requirements in all areas that relate to security
2. Authenticates (if necessary) only over secure channels
3. Transfers protected data only over secure channels
4. Avoids storing protected data on web or application servers unless this is required to meet specified functionality, and encrypts all protected data that must be stored (if protected data is to be stored, its nature and extent must be provided to the Information Security Office)
5. Deals with unexpected inputs, modification of session cookies, or other unusual conditions in a manner that does not weaken application security
6. Maintains a secure system state through all initializations, shutdowns, and aborts
7. Uses established methods to deter security exploits

I&IT Web Development should be consulted early in the development process to facilitate compliance with the university World Wide Web policy and accessibility requirements. Comprehensive testing, including tests for commonly known exploits, must be completed before the application is released into a production environment. Application developers should review the OWASP Top Ten, which represents a broad consensus about what the most critical application security flaws are. Test plans and results should be documented. Protected data must not be displayed in any user documentation. Previously deployed applications must be tested as part of any significant upgrade or as indicated by risk assessment. The Information Security Office should be consulted when the web application is designed to handle or manage protected university data.

Protected data should not be used for testing or development purposes, except where required to meet specified functionality. If protected production data must be used in a non-production environment, then security controls in the nonproduction environment must be as strong as the security controls in the production environment.

Procedures for deployment of code and data to production environments

To establish a stable, protected production system, application developers are expected to maintain a multi-tier environment, ideally containing at least three levels:

1. Development—Initial application development and testing, initial development and testing of application upgrades and functional changes.
2. Quality Assurance (“Testing”)—Final technical and security testing; functional testing by staff or end-users, as appropriate; testing of changes to web page content.
3. Production—Public-facing application with all functionality and security fully tested. Code will be changed on production servers only within the change control process, or under exceptional circumstances to remediate outages or avoid data loss or compromise; in the latter case, all changes will be fully documented as soon as practical after the change.

Developers must follow documented procedures for moving code and data into production. Projects will not be moved into the production environment until:

- All test data and test accounts are removed
A compliance and security review is completed for all new or significantly modified applications.

The compliance review will address:
- Campus World Wide Web Policy
- Accessibility Requirements

The security review will consider:
- Common security flaws - OWASP Top Ten

If the application handles protected data, the application will also be assessed by the Information Security Office using automated application vulnerability assessment tools.

Procedures for user acceptance and deployment
Developers should supply appropriate documentation when deploying an application. The documentation should detail specific configuration requirements for the application, including necessary ports, protocols and services, and operational procedures (this is especially important if the application uses non-standard ports or protocols). If the application handles protected data, then details regarding secure access and storage should be specified. Such documentation may include explicit designation of personnel who will be using the application, including any prerequisite training, security issues or other special requirements.

Finally, Division IT Management will ensure that, as long as the application is in use, maintenance will be available to address any security flaws subsequently discovered.

External web application development and off the shelf web applications purchased for use on the University network

All requisitions, contracts, service level agreements, and memoranda of understanding executed with third parties developing web applications on behalf of the University or its Auxiliaries will contain specific language guaranteeing to secure systems and data according to the University Web Application Code Development Standards.

Before an off-the-shelf web application is purchased for use on the University network a compliance and security review needs to be completed to ensure that the web application abides by the University Web Application Code Development Standard. The I&IT Vice President must review and approve the purchase to verify that the production environment is capable of supporting the application requirements and that the appropriate security controls are in place.
Procedures for deployment of third party software purchased off the shelf software systems to production environments

Web applications developed by external developers will not be moved into the production environment until they are formally reviewed and approved by I&IT:

- A security review is completed for all new or significantly modified applications
  - A security review will consider:
    - Common security flaws - OWASP Top ten

If the application handles protected data, the application will also be assessed by the Information Security Office using automated application vulnerability assessment tools.
References

The following documents were used in the construction and development of the standard.

Building Secure ASP.NET Applications: Authentication, Authorization, and Secure Communication

Cal Poly Pomona Information Classification and Handling Standard

Chico State Web Application Development Standard

Improving Web Application Security: Threats and Countermeasures

The Open Web Application Security Project (OWASP) Top Ten Project

OWASP Development Guide

PCI Payment Application Data Security Standards
https://www.pcisecuritystandards.org/pdfs/pci_pa_dss.pdf