

Secure Web Apps Team Meeting

Attendees: Listed at end of document

Meeting Date: January 26, 2006

Meeting Topic:

Handouts:

OWASP #1	A1	Unvalidated Input
OWASP #2	A2	Broken Access Control
OWASP #3	A3	Broken Authentication and Session Management
OWASP #4	A4	Cross-Site Scripting (XSS) Flaws

Minutes:

- Susan Kennedy started meeting with an overview of the Agenda
- The Secure Web App website has been created by John Lupton and there have been no problems reported with PennKey access by the team. As a reminder,
 - All files should be sent to Susan Kennedy for review and then to John Lupton for uploading to the website. John prefers Acrobat file format but will convert any other format to Acrobat if necessary. It was agreed that Acrobat would be the best format to use on the Web for documents.
 - The website URL is: <http://www.upenn.edu/computing/security/swat> . Login to the website will be by PennKey.
 - Version number and revision date should be included on all documents that are added to the website.
 - Don't forget to start sending any relevant documentation/best practices you already have drafted for the "miscellaneous" section of the website.
- A question was brought up at an earlier meeting regarding copyright issues and updating the OWASP documents. Is it our basic goal to modify by adding to the standards for Penn/UPHS specifics. The following copyright and license info is from one of the documents on the website, [A Guide to Building Secure Web Applications and Web Services; 2.0 Black Hat Edition; 7/27/2005.](#)

Copyright and license

© 2001 – 2005 Free Software Foundation.

The Guide is licensed under the Free Documentation License, a copy of which is found in the Appendix. PERMISSION IS GRANTED TO COPY, DISTRIBUTE, AND/OR MODIFY THIS DOCUMENT PROVIDED THIS COPYRIGHT NOTICE AND ATTRIBUTION TO OWASP IS RETAINED.

OWASP #1	A1	Unvalidated Input
-----------------	-----------	--------------------------

- Section A1.1 – To continue to work on the wording for the risks.
- Section A1.2 – Stephen Kratowicz prepared a grid of available tools for checking for unvalidated input (OWASP Item A1) across different platforms. The platforms included: PHP, ASP.NET, J2EE, and Perl. **Additional information for Cold Fusion will be added.**
- Section A1.4 – Along with information added from last meeting the last item was added.
 - 1. Global Variables Exploit w/Post and Get – initialize global variables
 - 2. Cross-site Scripting – this is a universal attack, script tags is a well known function

- 3. SQL Injection – use binding, if not use strings or integers (put integers in quotes)
- 4. Validate where the URL is input from a field in a form.
- 5. Encode data before echoing it back to the browser.

OWASP #2	A2	Broken Access Control
-----------------	-----------	------------------------------

- Section A2.2 – Several discussions regarding the use of server versus web application authentication. **Add definition of Local authentication and server authentication vs. authorization.** The following has been added into this section: (or needs to be relocated to the correct section)
 - UPHS: For Medview, a user has a NT account or a separate account for Medview. Currently evaluating other internal integration strategy.
 - Use PennKey when possible. **Further work to be done here to identify instance for authorization outside of Penn for those that don't have a PennKey.**
 - **Websec versus application authentication**
- Section A2.5 – How to Protect Yourself – discussion items.
 - Check authorization on every page.
 - Example of the URL being changed therefore must validate on each input.
 - Do not inadvertently become a proxy. Careful input checking.
 - Only allow short amounts of time for token sessions. **(Suggested timeframe?)**
 - Destroy token on server side.
 - Remove all demo code
 - Change defaults
 - Force random session IDs

Roberto is drafting examples of Insecure Id's and Forced Browsing sections.

OWASP #3	A3	Broken Authentication and Session Management
-----------------	-----------	---

- Section A3.2 – Several discussions regarding the use of server versus web application authentication. The following has been added into this section:
 - Websec is good to use but many are not using a logout mechanism to destroy tokens therefore the risk is someone could take your token and login to your session again. The Guidelines for PennKey system should be expanded.
 - Token is independent of the browser.
 - Should expire session token on the server and destroy it when browser is closed.
 - Do not write your own routines to authenticate, end sessions, tokens, etc., use the tool's functionality.
 - One session token (1st key) and one application token (2nd key)
 - **Need to include examples of how to check for when a “back browser” action is taken or use of an expiring timestamp.**
 - PennKey used for authentication only. Does not determine access needs.
 - PennKey proves who you are, not what you can do.
 - Do not use higher privileges than are necessary.
 - File permissions – limits
 - Web applications should run using a “low security account”.
 - Authentication (does not expire, i.e. PennKey) versus authorization (must expire).
 - Gold card authentication used by the Library i.e. CHUP
 - SecureIDs
 - PennCard IDs

- Do not allow users to set their own session Ids. Force a “sufficiently random” session. Length? It is not recommended to use a time stamp or other sequential formula. Concept of globally unique modifier.
 - Do not use timestamp as token. Can use timestamps associated with IDs – just not as a stand alone check.
 - Do not use any data value that is guessable.
- Verify the session. Do not trust IP addresses. DSL tend to change IP address. If dial-up user, most likely to have an odd IP address. AOL users IP address change during the session.
- Trust relationships, notes are not clear but appear to say do not rely on these. Need to draft an example.
- Do not embed data base or other IDs and/or passwords in the code.
- Do not enumerate account lists.
- If the web server is within a shared environment (multiple services on the same server), do not allow sharing of directories. Verify that permissions are set up correctly.
- Path traversal – remove all demo code
- Verify that the server configuration is proper for your environment. Do not accept the server defaults without analysis. Defaults are usually bad.
- User account management:
 - Include or link to best practices for user account management, i.e. annual account review using active personnel list or files; if user has not logged in for a specified period of time, disable/deactivate.
 - Do not use generic user accounts
 - MUST not use generic administrator accounts
 - Use different administrator accounts and passwords for each server
- Server security management:
 - Privileges and administrative interfaces. Do not use elevated privileges.
 - Limit access to administrators and only use “secure shell” or console privileges.
 - Authenticate for all levels.
 - Use audit trails and logging. Preferably log to a log server.
 - Do not allow users to use “Webmend” as well as other administrative functions.

OWASP #4	A4	Cross-Site Scripting (XSS) Flaws
-----------------	-----------	---

- To be continued.
- Next meeting is February 23, 2006 1:00-2:00PM, Samson West, room 306 Bits & Pieces

Secure Web Application Coding Team Members

	Raymond Bokenkamp	rbokenk@mail.med.upenn.edu	215-746-0103
	Chris Blickley	blickley@hr.upenn.edu	215-898-6162
	Doug Brunk	brunk@mail.med.upenn.edu	215-573-0253
√	Eric Chen	emchen@isc.upenn.edu	215-573-7550
√	Jim Choate	choate@isc.upenn.edu	215-898-4709
	Chris Filippone	cff@dental.upenn.edu	215-898-8957
√	Christopher Herdt	cherdt@law.upenn.edu	215-898-9140
√	Dan Hill	dwhill@pobox.upenn.edu	215-662-6332
	Bil Kasenchar	bm@pobox.upenn.edu	215-898-0001
	Ian Kelley	ikelley@pobox.upenn.edu	215-573-5243
√	Susan Kennedy	susanken@pobox.upenn.edu	215-573-4495
√	Stephen Kratowicz	kratowis@uphs.upenn.edu	215-349-8441
√	John Lupton	lupton@isc.upenn.edu	215-573-3811
√	Roberto Mansfield	robertom@sas.upenn.edu	215-573-4712
√	John Ockerbloom	ockerblo@pobox.upenn.edu	215-573-0758
√	Dominic Pasqualino	dominicp@pobox.upenn.edu	215-898-1933
	Steven Rosato	stevenjr@pobox.upenn.edu	215-898-4294
	Terrence Ryan	tpryan@wharton.upenn.edu	215-898-6705
	Matt Snyder	mwsnyder@law.upenn.edu	215-573-5498

√ indicates in attendance on 1/26/2006