Secure Web Apps Team Meeting

Attendees: Listed at end of document

Meeting Date: December 1, 2005

Meeting Topic:

Handouts: OWASP #1 A1 Unvalidated Input
OWASP #2 A2 Broken Access Control

Minutes:

• Introductions

• Agreed that team name is Secure Web Apps Team

• Doug Brunk and Ray Bokenkamp discussion for SOMIS web development

  PHP, PERL, Oracle backend database
  SOM uses Oracle server database and the data warehouse
  SOMIS has 10 web developers

  Have developed 3 logical areas for web apps.
  Layers are:
  1. WI Engine
  2. LDL or Logical Data Area
  3. Oracle Server

  WI Engine –
  Gateway for all web apps
  Delegates all queries to appropriate tool
  Takes care of all security requirements prior to retrieving data
  Assures authentication happens
  After authentication, enforces what panel a user can see
  Handles encryption if needed
  Handles reloads
  Determines what panels a user can access
  SSL enforcement

  LDL –
  Is an API (application program interface)
  A layer above the data
  PHP
  CRUD create read update delete
  Gateway for data in and out
  Would take care of SQL injection, etc
  Do form evaluation
  Form element security
  In LDL can apply rules to the data that must be enforced
  All business logic is stored here
  Some rules can be used within WI and LDL
  Various security levels – role level, column level
For change management: enforced by LDL
Using XML
Definitions in LDL

WI engine has html templates
SMARTY for PHP used for the templates

Once past LDL, could get into Oracle

SOMIS Web group is converting the Oracle interface so that a user logs into Oracle as an anonymous user, then the application procedures run to elevate access (authentication) and stores internally the authenticated user account, name and roles

- Terrence Ryan, discussion for Wharton Computing web development

Eleven (11) full time developers plus approximately 20 others who perform web work (Wharton computing staff has approximately 100 personnel.)

Use a 2-server configuration.
- Developer staging
- Production server
These are the same server but users view it as if they are 2 different servers.

All web application coding must go through a code review phase prior to it being moved into the production environment. Every line of code is reviewed and every development type. Sequel, ASP, ColdFusion all included.

Wharton uses a “developer center”. Coders can post onto Blogs. Coders are encouraged to share their code.

How Wharton “sells” the code review:
- Make sure code is good
- Learn from other people
- To show off, example cited was one of the first to use RSS

The code reviewers follows a standard of practice:
1 – have to change, example a “select *”
2 – use of variables, etc. “stylistic concerns”
3 – performance, depending on how many people would use the application, a middle ground is usually agreed to

Wharton has developed a “review guideline sheet”, this includes items such as
- every table has to have an index
- broiler plates, script to authenticate to the Wharton domain; ColdFusion 7.0 – flash siglets that assist the developers
- Blog is the main method to share information

- Discussed the topics for the Technical Standards template. The team agreed to the 5 headings that OWASP uses, but suggested that we add more examples that are specific to Penn and multiple development environments (highlighted below in blue text):

  1.  Description
• The group decided to add these two additional points in this section:
  i. Related Vulnerabilities
  ii. Risk

2. Environments Affected
• The team decided to add these two additional points in this section:
  i. Matrix summarizing the types of tools available (for each language) to identify known vulnerabilities that are particular to that specific language.
    1. Strengths and weaknesses within each tool w/ examples
  ii. Server configuration best practices

3. Examples and References

4. How to determine if you are vulnerable
• The group wants to add more detail for “How to Exploit”

5. How to protect yourself
• The group wants to add these details:
  i. Code Samples – Specific to development language
    1. Good and Bad Code
  ii. Suggested Libraries

• The team discussed the content of OWASP A1 Unvalidated Input.
  • Tasks:
    i. Section A1.1 Description - Susan Kennedy to write up additional risks associated with unvalidated input.
    ii. Section A1.2 Environments Affected - Steve Kratowicz to make a grid of available tools for protecting against malicious input by development platform.
    iii. Section A1.4 - How to Determine If You Are Vulnerable - Terry Ryan to write up an Cold Fusion example and Ray Bokenkamp will write up a PhP example.
    iv. Section A1.5 How To Protect Yourself – Everyone to develop 1-2 examples.
    v. Susan Kennedy – to add the examples/documentation to the Penn Technical Standard documentation once everyone completes their task.

• Time did not allow for discussion on A2 Broken Access Control so this will be discussed at next meeting.

• Next meeting is January 12, 2006 1:00-2:00PM, Samson West, room 306 Bits & Pieces
<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joshua Beeman</td>
<td><a href="mailto:jbeeman@isc.upenn.edu">jbeeman@isc.upenn.edu</a></td>
<td>215-573-6798</td>
</tr>
<tr>
<td>Raymond Bokenkamp</td>
<td><a href="mailto:rpbokenk@mail.med.upenn.edu">rpbokenk@mail.med.upenn.edu</a></td>
<td>215-746-0103</td>
</tr>
<tr>
<td>Chris Blickley</td>
<td><a href="mailto:blickley@hr.upenn.edu">blickley@hr.upenn.edu</a></td>
<td>215-898-6162</td>
</tr>
<tr>
<td>Doug Brunk</td>
<td><a href="mailto:brink@mail.med.upenn.edu">brink@mail.med.upenn.edu</a></td>
<td>215-573-0253</td>
</tr>
<tr>
<td>Eric Chen</td>
<td><a href="mailto:emchen@isc.upenn.edu">emchen@isc.upenn.edu</a></td>
<td>215-573-7550</td>
</tr>
<tr>
<td>Jim Choate</td>
<td><a href="mailto:choate@isc.upenn.edu">choate@isc.upenn.edu</a></td>
<td>215-898-4709</td>
</tr>
<tr>
<td>Chris Filippone</td>
<td><a href="mailto:cff@dental.upenn.edu">cff@dental.upenn.edu</a></td>
<td>215-898-8957</td>
</tr>
<tr>
<td>Aimee Gomez</td>
<td><a href="mailto:agomez@pobox.upenn.edu">agomez@pobox.upenn.edu</a></td>
<td>215-573-4854</td>
</tr>
<tr>
<td>Christopher Herdt</td>
<td><a href="mailto:cherdt@law.upenn.edu">cherdt@law.upenn.edu</a></td>
<td>215-898-9140</td>
</tr>
<tr>
<td>Dan Hill</td>
<td><a href="mailto:dwhill@pobox.upenn.edu">dwhill@pobox.upenn.edu</a></td>
<td>215-662-6332</td>
</tr>
<tr>
<td>Bil Kasenchar</td>
<td><a href="mailto:bmk@pobox.upenn.edu">bmk@pobox.upenn.edu</a></td>
<td>215-898-0001</td>
</tr>
<tr>
<td>Ian Kelley</td>
<td><a href="mailto:ikelley@pobox.upenn.edu">ikelley@pobox.upenn.edu</a></td>
<td>215-573-5243</td>
</tr>
<tr>
<td>Susan Kennedy</td>
<td><a href="mailto:susanken@pobox.upenn.edu">susanken@pobox.upenn.edu</a></td>
<td>215-573-4495</td>
</tr>
<tr>
<td>Stephen Kratowicz</td>
<td><a href="mailto:kratowis@uphs.upenn.edu">kratowis@uphs.upenn.edu</a></td>
<td>215-349-8441</td>
</tr>
<tr>
<td>John Lupton</td>
<td><a href="mailto:lupton@isc.upenn.edu">lupton@isc.upenn.edu</a></td>
<td>215-573-3811</td>
</tr>
<tr>
<td>Roberto Mansfield</td>
<td><a href="mailto:robertom@sas.upenn.edu">robertom@sas.upenn.edu</a></td>
<td>215-573-4712</td>
</tr>
<tr>
<td>David Millar</td>
<td><a href="mailto:millar@isc.upenn.edu">millar@isc.upenn.edu</a></td>
<td>215-898-2172</td>
</tr>
<tr>
<td>John Ockerbloom</td>
<td><a href="mailto:ockerblo@pobox.upenn.edu">ockerblo@pobox.upenn.edu</a></td>
<td>215-573-0758</td>
</tr>
<tr>
<td>Dominic Pasqualino</td>
<td><a href="mailto:dominicp@pobox.upenn.edu">dominicp@pobox.upenn.edu</a></td>
<td>215-898-1933</td>
</tr>
<tr>
<td>Steven Rosato</td>
<td><a href="mailto:stevenjr@pobox.upenn.edu">stevenjr@pobox.upenn.edu</a></td>
<td>215-898-4294</td>
</tr>
<tr>
<td>Terrence Ryan</td>
<td><a href="mailto:tpryan@wharton.upenn.edu">tpryan@wharton.upenn.edu</a></td>
<td>215-898-6705</td>
</tr>
<tr>
<td>Matt Snyder</td>
<td><a href="mailto:mwsnyder@law.upenn.edu">mwsnyder@law.upenn.edu</a></td>
<td>215-573-5498</td>
</tr>
<tr>
<td>David Taylor</td>
<td><a href="mailto:ltr@isc.upenn.edu">ltr@isc.upenn.edu</a></td>
<td>215-898-1236</td>
</tr>
<tr>
<td>Peggy Yetter</td>
<td><a href="mailto:yetter@isc.upenn.edu">yetter@isc.upenn.edu</a></td>
<td>215-573-7257</td>
</tr>
</tbody>
</table>

√ indicates in attendance on 12/1/2005