Secure Web Application Coding Team
Introductory Meeting
November 15, 2005
1:30 – 3:00PM

Agenda

1. Introductions
2. Discuss and identify:
   a. Team objectives/goals --- what are we going to do?
   b. Methodology for developing secure web application coding standards and
      best practices for the institution at large --- how are we going to do it?
      i. Drivers for standards could be OWASP, existing standards,
         combination, etc.
   c. Deliverables --- what are we creating?
   d. Timeline --- when are we going to have deliverables?
   e. Communication Channels --- where are we going to communicate our
      deliverables?
   f. Responsibilities --- who is responsible?
3. Meeting Logistics
   a. Frequency and Timeframe of Meetings
   b. Location
4. Current Development Procedures at Penn
   a. ISC
   b. SOM
   c. Others?
5. Industry Tool
   a. OWASP
6. Some recent vulnerabilities within Penn that have been identified:
   a. Re-authentication & the browser back button
   b. Parameter manipulation/Directory Traversal
   c. Password Encryption
   d. Session ID Management
   e. Validation of data input
7. Some Security Testing Tools:
   a. WebInspect
   b. Nitko
   c. Paros
   d. Cookie Digger
   e. Site Digger