Security Injections
Workshop – January 2010

Anne Arundel Community College
Bowie State University
Community College of Baltimore County
Harford Community College
Towson University
Today's Goals

- Project Overview
- Security Injection Details
- How can you participate?
- Project Results
- Feedback
Agenda

• 10:00  Introductions
  Project Overview
  Security Injection Details/Process Results

• 11:30  Discussion
  Questions?
  What does it take to get this model to be useful?
  What works? What doesn't?
  How do we make these materials more effective?
  Encourage others to use them?

• 12:00  Lunch

• 12:45  Schedule
  Wrap-up
Introductions

- Develop & Pilot
  - TU - Blair, Sidd, Shiva, & Mike
  - Bowie - Claude
- Deploy
  - AACC - Trish
  - Harford - AC
  - CCBC - Jack
- TU and BSU assess and revise
- MAISA recreates
Overview
Project Goals and Motivations

• Importance of Security
• Security Tracks and classes
  – Too little too late
  – Insecure coding techniques
• Security Injections
  – Early and often
  – Minimally invasive
Overview
Security Injection Modules

• Secure coding “big three”
  – Integer overflow
  – Buffer overflow
  – Input validation

• CIS0 (Computer Literacy)
  – Phishing
  – Passwords
  – Cryptography

• Format of modules
  1. Background - description, risk, examples
  2. Lab Assignment
  3. Checklist
  4. Discussion Questions
  – Java/C++ versions

• http://darwin.towson.edu/~cssecinj/
Security Injection Details

- CS0, CS1, & CS2 (Blair)
- CIS0 (Computer Literacy) (Claude)
- Dbase (Shiva)
- Web – *coming Fall 2010 at TU*
- Networking – *coming Fall 2010 at BSU*
Process - How can you participate?

http://darwin.towson.edu/~cssecinj/

1. Administer Security Survey
2. Introduce Security Injections in class
3. Administer Security Survey
4. Complete Faculty Survey
Results

• Outreach
  – 2008-2009 – 16 sections
  – Workshops
    • Summer workshop – 12 new participants
    • TU – CIS0 – 3 new participants
    • Jan workshop – ? new participants
    • Feb – Bowie
  – Presentations

• Quantitative Results - mixed
  – Between sections, no significant improvement
  – Next analysis – summer 2010
  – CS0 - Split section – still being analyzed
  – Posttest scores for CS0-CS2 students significantly higher than graduating seniors

• Qualitative
  – Students find checklists easy to use
  – More discussion?
Progress from Year 1: Survey - 534 Responses

• 23 sections, 16 integrated.
  - CS 0 3/3
  - CS 1 5/7
  - CS 2 3/5
  - CIS0 1/5

• Student Institutions
  - Bowie State 13.2%
  - CCBC 5.6%
  - Harford CC 11.4%
  - Towson 69.6%

• Student Gender
  - Male 70%
  - Female 30%

• Student Ethnicity
  - White 58%
  - Black 26%
  - Asian 7%
  - Hispanic 2%
  - Other 6%

• Student Standing
  - Freshman 26%
  - Sophomore 29%
  - Junior 28%
  - Senior 12%
  - Other 5%

• Student Major
  - Computer Science 25.3%
  - Computer Info Sys 29.4%
  - Math 6.3%
  - Undecided 3.4%
  - Other 35.0%
## Progress from Year 1

### Pretest→posttest data

<table>
<thead>
<tr>
<th>Class</th>
<th>PRE</th>
<th>POST</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>9.47</td>
<td>11.06</td>
</tr>
<tr>
<td>All S</td>
<td>10.1</td>
<td>11.33</td>
</tr>
<tr>
<td>CS0S</td>
<td>9.16</td>
<td>11.02</td>
</tr>
<tr>
<td>CS1</td>
<td>8.23</td>
<td>10.5</td>
</tr>
<tr>
<td>CS1S</td>
<td>10.28</td>
<td>11.49</td>
</tr>
<tr>
<td>CS2</td>
<td>11.07</td>
<td>11.75</td>
</tr>
<tr>
<td>CS2S</td>
<td>11.53</td>
<td>11.94</td>
</tr>
</tbody>
</table>

![Graph showing pretest vs posttest scores for different classes.](chart.png)
Results
Faculty Surveys

• 13 faculty for spring 09 and fall 09
1. How would you rate the student interest in the security materials?
   Not very interested 1  2  3  4  5   Extremely interested
   ➢ Most answered between 3 and 4
2. How well were you able to incorporate these materials in your class?
   Very troublesome 1  2  3  4  5   No problems at all
   ➢ Most answered between 4 and 5
3. Did time spent on these topics take detract from other topics that you might have covered?
   Not at all 1  2  3  4  5   Significantly
   ➢ 10/13 answered 1
4. Did the materials help you with your level of confidence in teaching the security concepts?
   • Not at all helpful 1  2  3  4  5   Very helpful
   ➢ All felt the materials helped their level of confidence
5. Would you recommend these materials or this approach to a colleague?
   Definitely not 1  2  3  4  5   Absolutely
   ➢ 10/13 answered 5
## Student feedback on checklists

<table>
<thead>
<tr>
<th>Statement</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>The checklists were easy to use</td>
<td>3.85%</td>
<td>26.92%</td>
<td>69.23%</td>
</tr>
<tr>
<td>The checklists helped me understand the concepts</td>
<td>8.00%</td>
<td>28.00%</td>
<td>64.00%</td>
</tr>
<tr>
<td>Checklists helped me understand vulnerabilities</td>
<td>12.00%</td>
<td>40.00%</td>
<td>48.00%</td>
</tr>
<tr>
<td>I would like to use checklists in future classes</td>
<td>17.39%</td>
<td>43.48%</td>
<td>39.13%</td>
</tr>
<tr>
<td>I liked the labs with checklists more than others</td>
<td>25.00%</td>
<td>45.83%</td>
<td>29.17%</td>
</tr>
<tr>
<td>I learned more from the labs with checklists</td>
<td>18.18%</td>
<td>40.91%</td>
<td>40.91%</td>
</tr>
<tr>
<td>The checklists increased discussion</td>
<td>26.09%</td>
<td>34.78%</td>
<td>39.13%</td>
</tr>
</tbody>
</table>
Progress from Year 1

What worked
• With the detailed background information, the students were able to work mostly on their own without having to spend a lot of class time discussing the issues.
• The idea that we can put them in the lab without much changes. I also liked that the injection was subtle without me talking to the class too much about it, they could link it to coursework implicitly.
• After multiple exposure to the checklists, students seemed to get the hang of it.
• In project after the topic, security was routinely brought up as something to make projects complete. So they are thinking about it

What didn’t
• timing was a problem
• Too long
• Many students (esp. CIS students) had a difficult time connecting the programming issues to what is really happening
• Students skipping background information
• One thing, you do not show "hints" or "working examples" that do work for some of the possible errors. (Only some)
Progress

How can we improve?

• More students + more institutions
• Getting faculty involved
• Feedback on modules
• Increase security awareness
• More split sections
• Specific exercises on quizzes/exams for content
Plans for Year 2

• CS0
  – Deploy TU
  – Pilot/Deploy BSU ?? (we are behind)
  – Pilot partners

• CS1
  – Deploy TU
  – Pilot/Deploy BSU
  – Pilot partners

• CS2
  – Pilot/Deploy TU
  – Pilot BSU

• CIS0
  – Pilot TU/Deploy BSU
  – Pilot partners
  – Pilot AACC

• CISDB
  – TU – pilot/deploy

• Summer 2010 – workshop at Harford?
Summary

• [http://darwin.towson.edu/~cssecinj/](http://darwin.towson.edu/~cssecinj/)
• materials for CS0, CS1, CS2
• CIS0 – computer literacy
• Future - Database, Web?
• Identify courses, sections
Questions

• Feedback
  – Changes to modules
  – Usage of modules
• Timing of modules
• Participation
  – How can we get colleagues to adopt?
  – What project/institutional support is needed?
  – Any issues specific to your context that we should know about?
• Brainstorm
  – Web
  – Database
Question (cont.)

• What topics would you recommend for web security:
  – cross-site scripting
  – injection flaws / SQL injection
  – insecure direct object reference
  – malicious file execution
  – cross site request forgery
  – broken authentication and session management
  – insecure cryptographic storage
  – insecure communications
  – failure to restrict URL access


• What languages?
  – PHP, Java, Rails, JSP, ASP .Net