Outline

Introduction

Artist eXchange Case Study
  Automated Testing
  Demo

Evaluation

Conclusions
Motivation

- Information technology is pervasive but cannot be trusted
  - Viruses, worms, and data theft are common
- Information security and computer security are popular topics (with good job prospects!)
- Security is a grand challenge in computer science
- CS community has obligation to educate computer scientists about professional and ethical responsibilities
Background

- Created “Laboratory for Electronic Commerce” with NSF DUE CCLI support in 2001–2003
  - Focused on hands-on e-commerce programming
  - Labs met Wednesdays 6–9 p.m.
    - Students dislike fixed lab times, want to work on their own schedule and at their own pace
    - Universal dislike of throwaway, independent exercises
- U.Va. supported the creation of virtual (i.e., web-based) labs
- NSF DUE CCLI support (NSF 06-536): “Secure E-Commerce: A Modular Course Supported by Virtual Laboratories”

Goal
Add security topics (both principles and practices) to the existing e-commerce course
Why practical security?

- Students fail to code securely
  - No whitelisting of valid input
  - No escaping user input
- Students don’t use security-related resources

Example

suPHP executes PHP script with the permission of its owner and allows all PHP files to be readable only by owner, but... students don’t use suPHP on shared web servers (passwords world readable!)
Why practical security?

- Students fail to code securely
  - No whitelisting of valid input
  - No escaping user input
- Students don’t use security-related resources

Example
suPHP executes PHP script with the permission of its owner and allows all PHP files to be readable only by owner, but... students don’t use suPHP on shared web servers (passwords world readable!)

```
[user@ includes]$ more config.php
<?php
  $dbhost = 'dbm1.itc.virginia.edu';

  $dbuser = 'qbg7r';
  $dbpass = 'cs4753';

  $dbname = 'qbg7r_website';
```
Artist eXchange

Case study patterned after popular social networking websites

- Artists create profiles
- Post pictures and music
- Users find artists and rate music samples

Objectives:
- Overview of common web technologies (e.g., HTML, JavaScript, PHP)
- Based on LAMP software stack
- Suitable for general introduction to web technologies
- Trivial to add additional technologies of interest to students (e.g., Flash)
Artist eXchange

Case study patterned after popular social networking websites

▶ Artists create profiles
▶ Post pictures and music
▶ Users find artists and rate music samples

Objectives:

▶ Overview of common web technologies (e.g., HTML, JavaScript, PHP)
▶ Based on LAMP software stack
▶ Suitable for general introduction to web technologies
▶ Trivial to add additional technologies of interest to students (e.g., Flash)
Artist eXchange (continued)

Objectives (continued):
▶ Exercises address common website vulnerabilities
  ▶ Correct functionality *and* common vulnerabilities checked via automated regression testing
▶ Students prefer assignments that build upon each other
  ▶ Case study currently includes 5 sequential labs
▶ End product: (simple, but) full-featured social networking website
Automated Testing

Integral part of Artist eXchange case study

Benefits:

- Real-time feedback on work
- Regression testing ensures changes do not break other functionality
  - Complete regression testing infeasible without automation
- Modularity provided by Selenium and TestNG
Automated Testing (continued)

Selenium RC (Remote Control)
- Automated web application UI tests designed for
  - Frequent regression testing
  - Rapid feedback during development
- Executes tests on student’s machine
  - Supports all mainstream JavaScript-enabled browsers
Automated Testing (continued)

TestNG
▶ Designed for the gamut of software testing, including integration tests
▶ Supports test dependencies
    ▶ Most test cases depend on the successful completion of other tests

Example
Test case for logging into website requires valid login form
Evaluation

Artist eXchange case study was well-received
- Students overwhelmingly rated the assignments as valuable and suggested they be retained in successive course offerings.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Positive %</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTML and JavaScript</td>
<td>77</td>
</tr>
<tr>
<td>PHP</td>
<td>91</td>
</tr>
<tr>
<td>MySQL &amp; PHP</td>
<td>91</td>
</tr>
<tr>
<td>File uploads</td>
<td>88</td>
</tr>
<tr>
<td>Website Security</td>
<td>82²</td>
</tr>
</tbody>
</table>

¹ No students rated an assignment negatively; the remaining percentage of students were neutral about the value of the lab.
² Many students requested more advanced security topics and sophisticated attack test cases than covered by the lab (e.g., more advanced than SQL injection, cookies vs. sessions, suPHP).
Evaluation (continued)

- Automated testing
  - Negative
    The testing system is not flexible.
  - Positive
    Online testing is glorious.
    ... liked the instant grade test cases
Evaluation (continued)

- Automated testing
  - Negative
    
    The testing system is not flexible.
  
  - Positive
    
    Online testing is glorious.
    
    ...liked the instant grade test cases

When asked about the best topics/activities from the course...

(Of course) the Artist eXchange website homeworks! Awesome design! + testing
Conclusions

- Virtual labs cater to students’ preference for flexibility when completing assignments
  - Frees university and teaching staff from holding fixed lab sessions
- Artist eXchange case study and assignments praised in evaluations
  - More advanced security topics and test cases for next course offering
- Automated testing minimizes time spent grading assignments, enabling faster feedback for students
- 43% of students protected against common threats *without being prompted to do so* on the final exam
  - Baseline for evaluating variant approaches in future course offerings
Thank You

Questions?