SWEET: Secure Web Development Teaching Modules

Team members: Li-Chiou Chen (PI), Lixin Tao (Co-PI), Chienting Lin, Pace University, New York
Xiangdong Li (PI), City College of Technology, City University of New York, New York

Introduction

Motivation: Web application security is critical to e-commerce, e-government and social networking but few text/labs are suitable for undergraduate students.

Goal: The goal is to enhance the learning experience of undergraduate students in computing through standardized teaching modules and environment in secure web development.

Expected Outcomes

- SWEET (**S**ecure **WE**b d**E**velopment **T**eaching), a set of portable modules to teach security practices in developing web application. SWEET can be downloaded from http://csis.pace.edu/~lchen/sweet/.
- Successful integration of SWEET in various computing courses.

Method

Virtualization Platform

- SWEET utilizes virtualization technology to configure a computing environment, as in Figure 1, needed for the hands-on laboratory exercises.

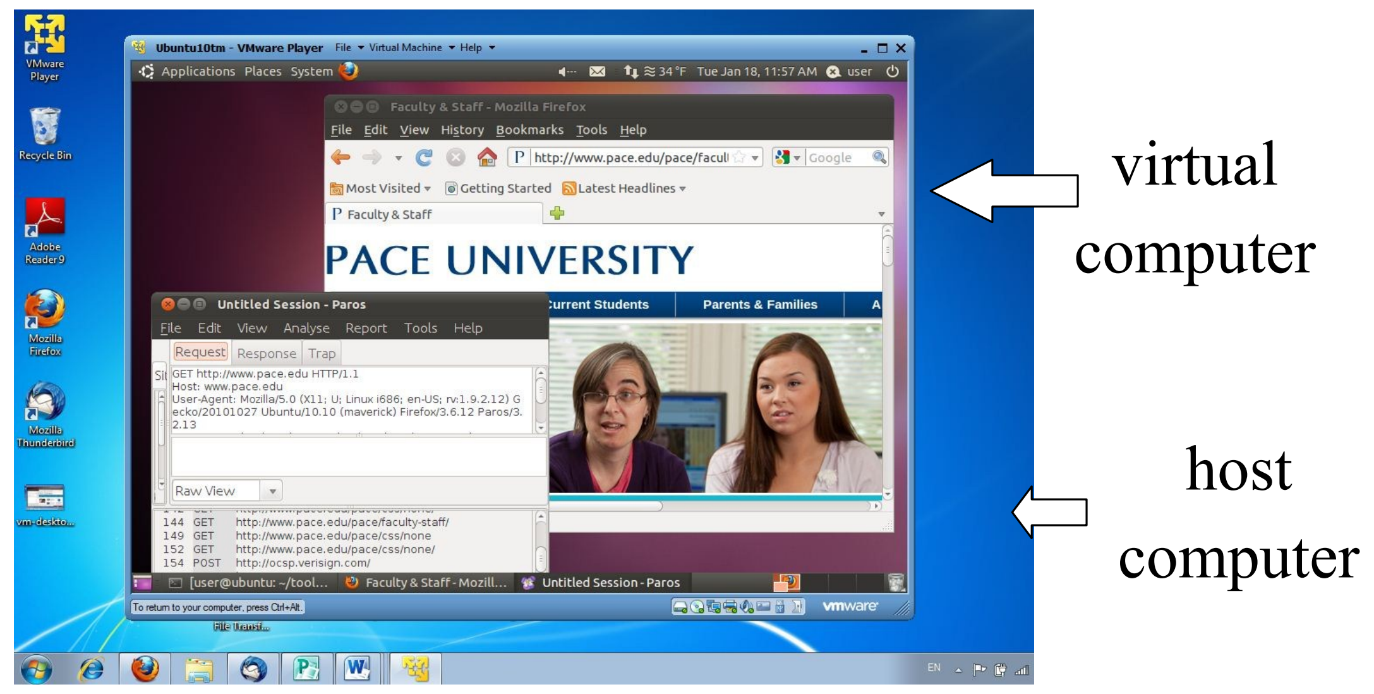


Figure 1. The Virtualized Computing Environment.

Software Architecture

- All software needed for SWEET modules is pre-installed on a Linux virtual computer. The virtual computer includes the following applications :
  - Web and application servers: Tomcat, Apache, Java,
  - Web proxy: Paros, Web Scarab,
  - Web security testing: Web Goat, a vulnerable web application (badstore.com)
  - Programming languages: Java, C#, C/C++, VB .NET , Perl, PHP, Ruby,
  - Programming IDEs: Eclipse, NetBeans, Visual Studio, JDK

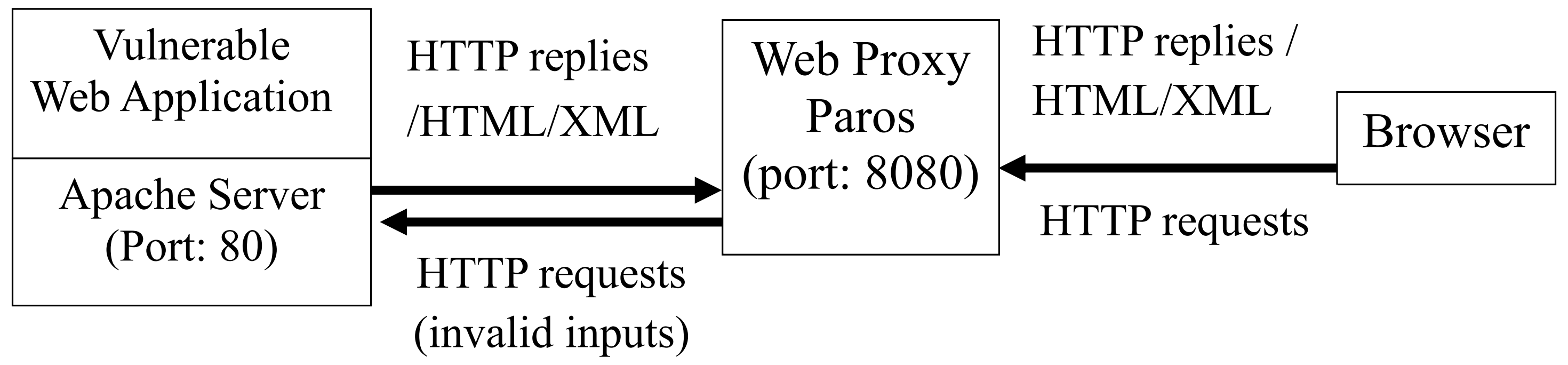
Outcomes

Audience

- Sophomore to junior undergraduate students who have only taken an introductory level of programming as well as some computer networking concepts.
- Information Systems/Information Technology Masters' students who have only an introductory background in computing.

SWEET Modules

- Each module introduces web application security or related concepts along with hands-on laboratory exercises illustrating the concepts. The modules include:
  - **Tutorials**: Linux overview, HTTP and HTML/XML .
  - **Teaching Modules**: web application development overview; service-oriented architecture overview, introduction to cryptography, secure web communications, threat assessment, security testing, vulnerability management, and Java security.
  - **Course Project Topics:** automatic web server scanning; online banking security; web application auditing.
  - **An example** : Figure 2 illustrates an example of a laboratory exercise to conduct security testing on a virtualized web server through the Paros web proxy.


Vulnerable Web Application

Apache Server (Port: 80)

HTTP replies /HTML/XML

HTTP requests (invalid inputs)

Web Proxy Paros (port: 8080)

HTTP replies / HTML/XML

HTTP requests

Browser

Figure 2. An Example of Security Testing.

Course Integration

- Each SWEET module is an independent topic. The modules can either be adopted separately in various courses or together in one course.
- We integrated SWEET into three different courses at Pace University and two different courses at New York City College of Technology.

Data Collection

- We collected data to evaluate SWEET over the past three semesters and will continue to collect for course integration information.
- Data collected include student feedback, faculty feedback, course integration information, and student performance through test questions and term projects.

Findings and Impacts

Preliminary Findings

- The table below lists the course information and the student responses of a web based survey (5: strongly agree and 1: strongly disagree).
- The survey questions included positive statements in four categories: lecture materials (mean: 4.10), laboratory exercises (mean: 4.15), mapping between lecture and lab (mean: 4.08), and overall impact of these modules on their learning experience and career (mean: 4.00).

Course name	Semester	Number of students	Number of student responses	Mean (Standard deviation)
Web Application Security	Fall 2009	47	30	3.97 (0.95)
Computer Security Overview	Fall 2009	20	14	4.34 (0.55)
Internet and Network Security	Spring 2009	11	10	4.35 (0.32)
Web Application Security	Fall 2010	45	40	4.13 (0.75)
Computer Security Overview	Fall 2010	34	28	3.92 (0.93)
Total		157	122	4.08 (0.81)

Impacts

- The survey results showed that the students invested a significant amount of time (1-3 hours/module on average) in completing their laboratory exercises, liked the modules, and were more interested than before in taking courses or pursuing a career in information assurance.
- Test questions and student projects provided evidence on the improvement of students' abilities in solving web security problems.
- SWEET modules were disseminated through conference presentations and workshops. Other academic institutions are currently testing the modules and plan for course integration.

Acknowledgement

This work is supported by NSF CCLI 0837549. The views and conclusions contained in this document are those of the author and should not be interpreted as representing the official policies, either expressed or implied, of the National Science Foundation or the U.S. government.