A Tool for Teaching Web Application Security

Li-Chiou Chen, Lixin Tao and Chienting Lin, Pace University
Xiangdong Li, City College of Technology, CUNY

The 14th Colloquium for Information Systems Security Education
06/07/2010

Outline

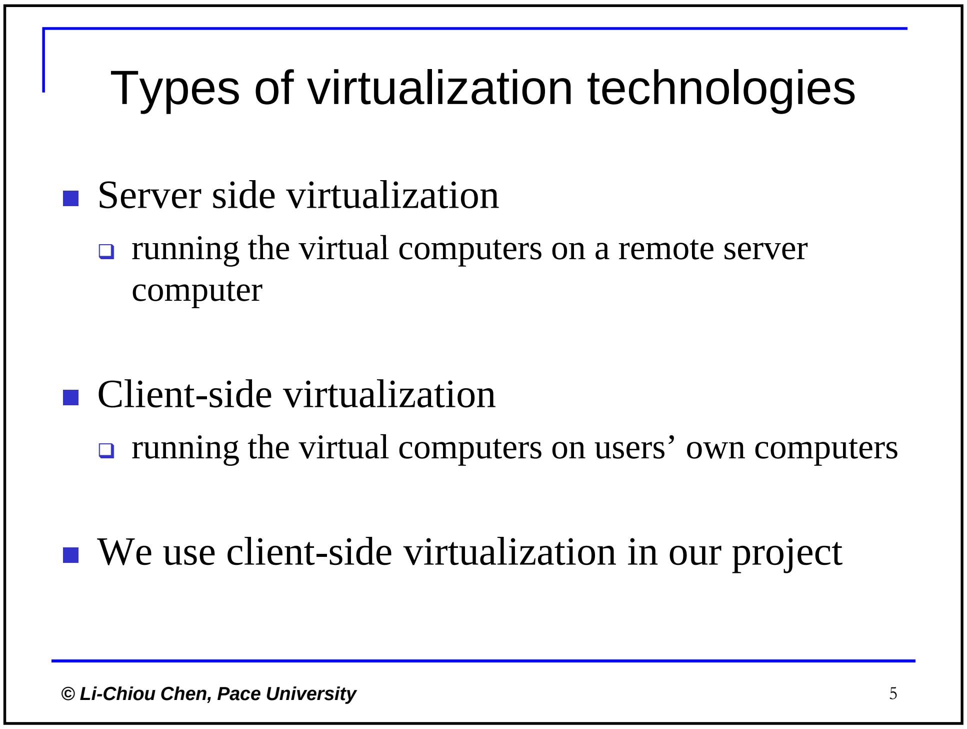
- Motivation
- Virtualization
- SWEET – Secure Web Application Development
- SWEET teaching modules
- Course adoption and evaluation
- Examples

Motivation

- Lack of Undergraduate Web Security Teaching Modules
  - Current web vulnerabilities and secure programming literature were designed for practitioners
- Aimed to design a new teaching tool called **SWEET (Secure WEb dEvelopment Teaching)**
  - For Undergraduate security curriculum
  - Software stack packaged in VMware virtual appliance
  - Installed in portable laboratories using laptops

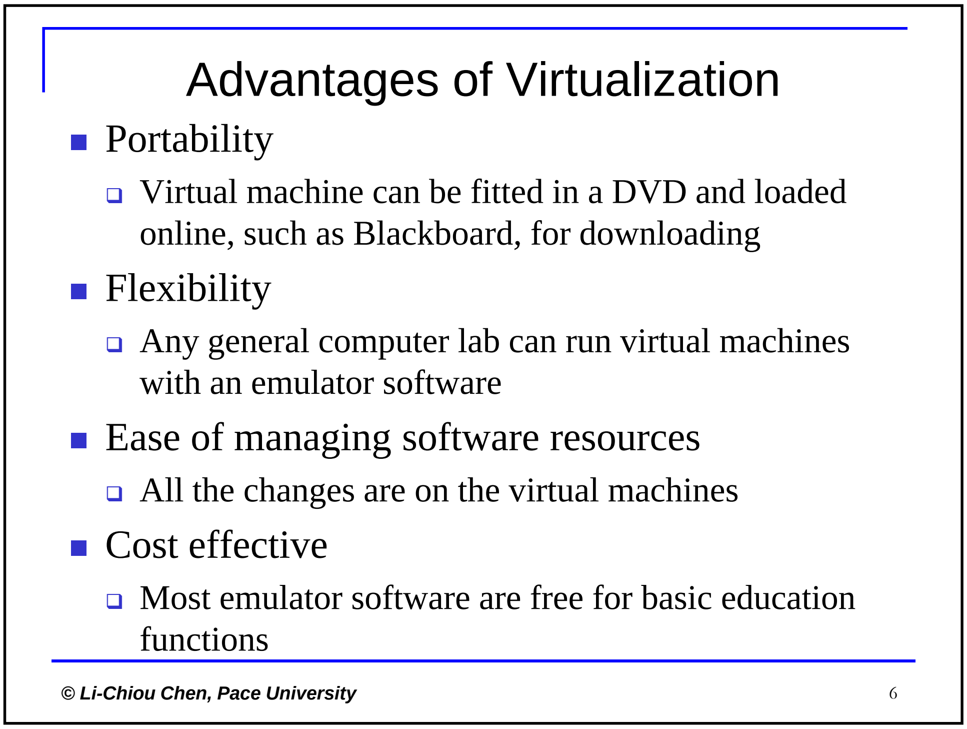
What is virtualization

- the virtualization of a computer means
  - To run one computer (virtual machine) on top another computer (host machine) within one physical machine
  - To use emulator software on the host machine
  - To emulate the computing environment of the virtual machine



Types of virtualization technologies

- Server side virtualization
  - running the virtual computers on a remote server computer
- Client-side virtualization
  - running the virtual computers on users’ own computers
- We use client-side virtualization in our project



Advantages of Virtualization

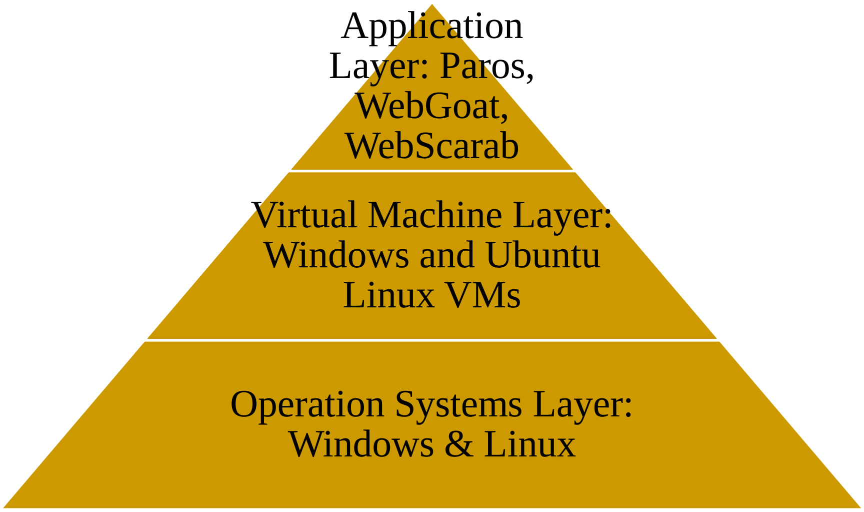
- Portability
  - Virtual machine can be fitted in a DVD and loaded online, such as Blackboard, for downloading
- Flexibility
  - Any general computer lab can run virtual machines with an emulator software
- Ease of managing software resources
  - All the changes are on the virtual machines
- Cost effective
  - Most emulator software are free for basic education functions

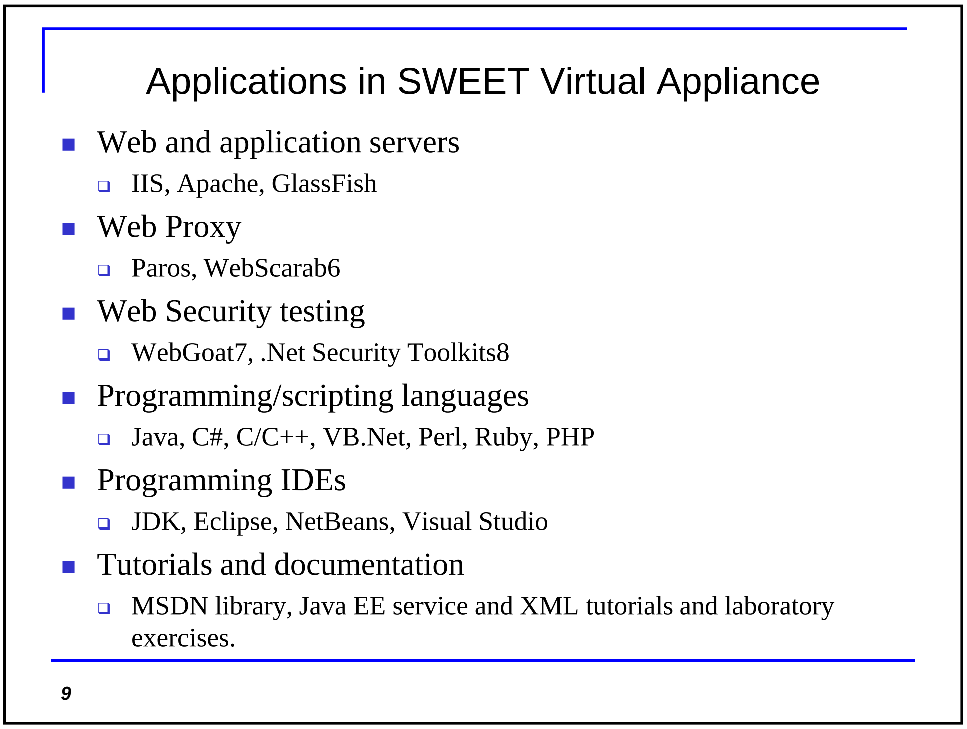
SWEET Project

- Pace University, Pleasantville & New York City, NY
  - Designated as a Centers of Academic Excellence in Information Assurance Education (CAEIAE) by the DOD and DHS (since 2004)
  - DOD-Supported security labs
  - Graduate IA Track in MS/IT and MS/IS Programs
  - Undergraduate IA Minor in conjunction with Criminal Justice
- CUNY City College of Technology
- OWASP (Open Web Application Security Project)
  NY/NJ Chapter serving as Industry Advisor

- Project web site: http://csis.pace.edu/~lchen/sweet

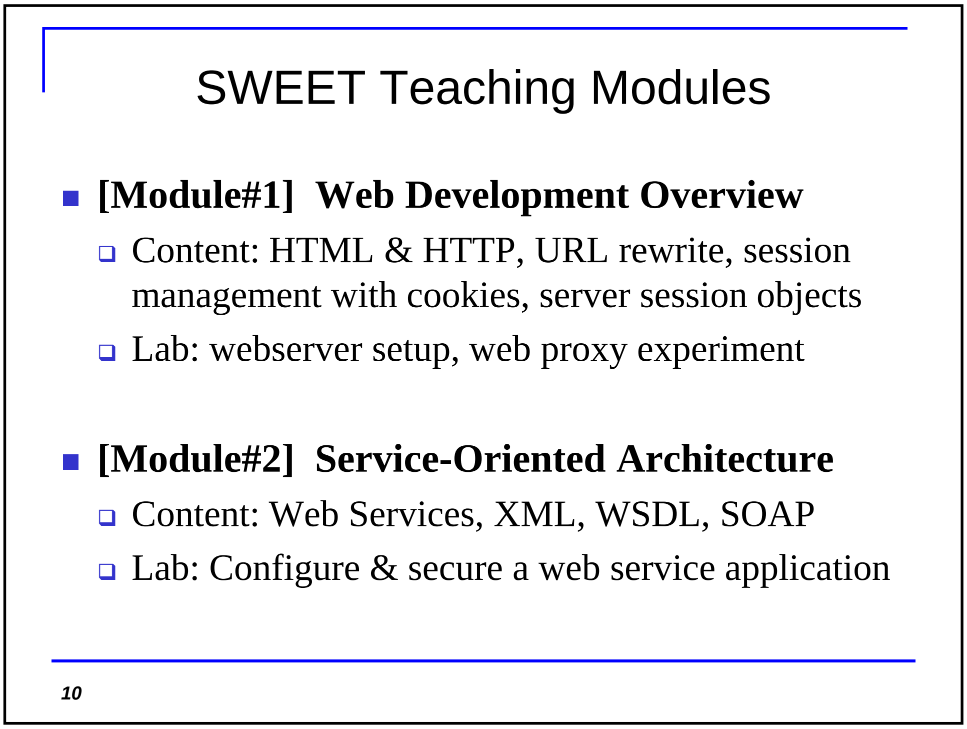
SWEET Architecture


Application Layer: Paros, WebGoat, WebScarab
Virtual Machine Layer: Windows and Ubuntu Linux VMs
Operation Systems Layer: Windows & Linux



Applications in SWEET Virtual Appliance

- Web and application servers
  - IIS, Apache, GlassFish
- Web Proxy
  - Paros, WebScarab6
- Web Security testing
  - WebGoat7, .Net Security Toolkits8
- Programming/scripting languages
  - Java, C#, C/C++, VB.Net, Perl, Ruby, PHP
- Programming IDEs
  - JDK, Eclipse, NetBeans, Visual Studio
- Tutorials and documentation
  - MSDN library, Java EE service and XML tutorials and laboratory exercises.



SWEET Teaching Modules

- **[Module#1] Web Development Overview**
  - Content: HTML & HTTP, URL rewrite, session management with cookies, server session objects
  - Lab: webserver setup, web proxy experiment
- **[Module#2] Service-Oriented Architecture**
  - Content: Web Services, XML, WSDL, SOAP
  - Lab: Configure & secure a web service application

SWEET Teaching Modules (cont'd)

- **[Module#3] Secure Web Communications**
  - Content: SSL, PKI/X.509, Online Certification Status Protocol (OCSP)
  - Lab: Configure SSL on a webserver to create & sign a server certificate
- **[Module#4] Secure Analysis & Design**
  - Content: Secure SDLC, CLASP, Abuse Case, Risk Analysis, Secure UML
  - Lab: Design a secure requirement plan & conduct a risk analysis

SWEET Teaching Modules (cont'd)

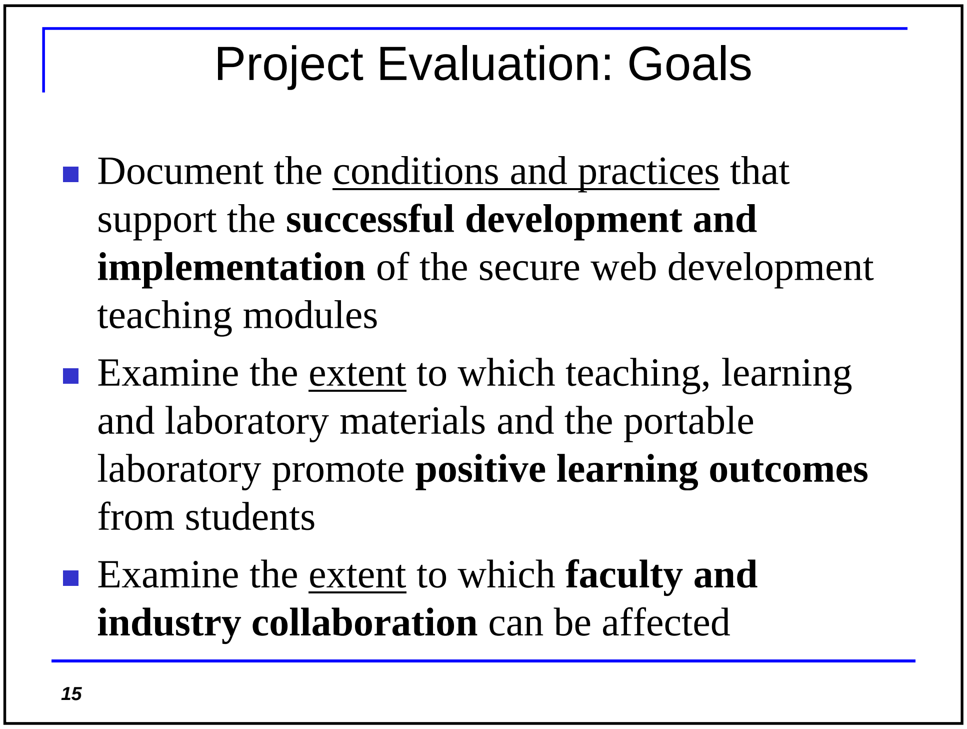
- **[Module#5] Secure Implementation**
  - Content: SQL injection, buffer overflow, poor authentication; Code Review, Risk-Based Testing
  - Lab: Hands-on testing on a vulnerable server
- **[Module#6] Secure Deployment**
  - Content: cross site scripting (XSS) and e-shoplifting; architectural risk analysis - attack resistance/ambiguity/weakness analyses.
  - Lab: Hands-on testing on a vulnerable server

SWEET Teaching Modules (cont'd)

- **[Module#7] Penetration & Stress Testing**
  - Content: Penetration testing, server load balancing, DDOS attacks
  - Lab: Plan & conduct a pentest on a web app
- **[Module#8] Securing AJAX Applications**
  - Content: client-side sandbox security, Java security policy management, securing AJAX applications
  - Lab: Study the vulnerabilities of a sample AJAX application

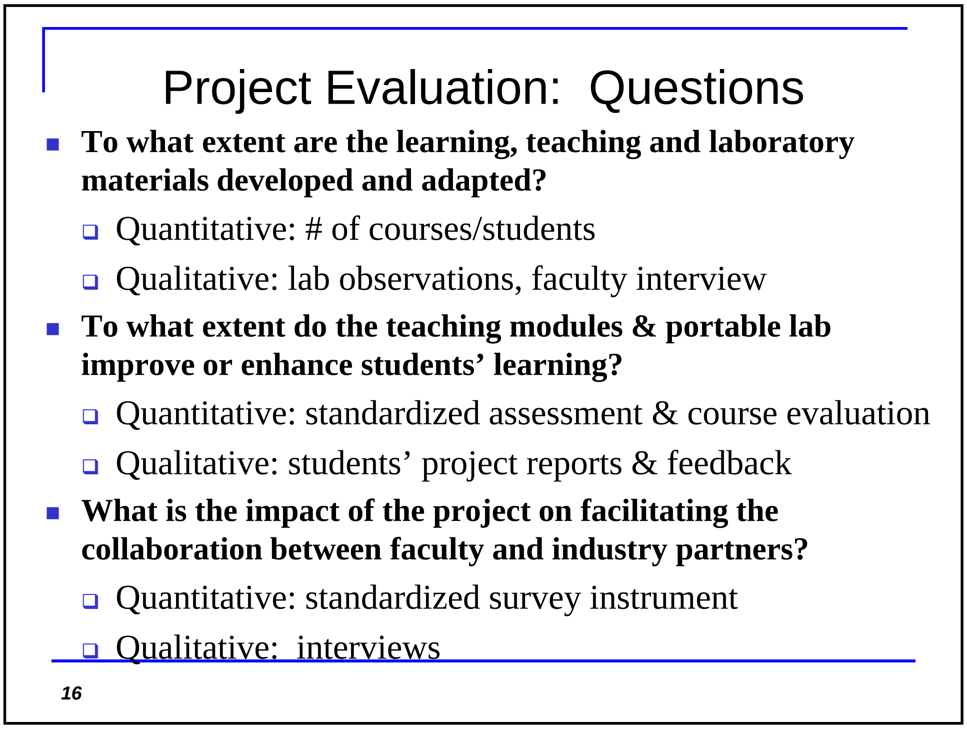
Course Adoption

- Overview of Computer Security
  - Undergraduate elective for BSIS and BSCS
- Internet and Network Security
  - Undergraduate elective for BSIS and BSCS
- Web Security
  - Graduate elective for MSIS and MSIT



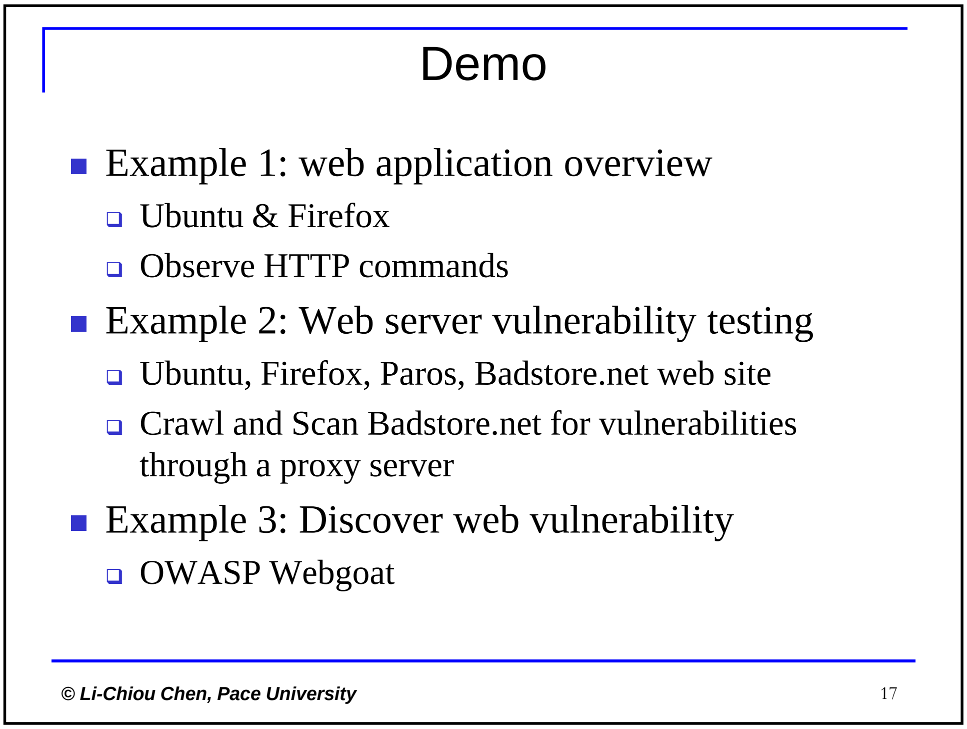
Project Evaluation: Goals

- Document the conditions and practices that support the **successful development and implementation** of the secure web development teaching modules
- Examine the extent to which teaching, learning and laboratory materials and the portable laboratory promote **positive learning outcomes** from students
- Examine the extent to which **faculty and industry collaboration** can be affected



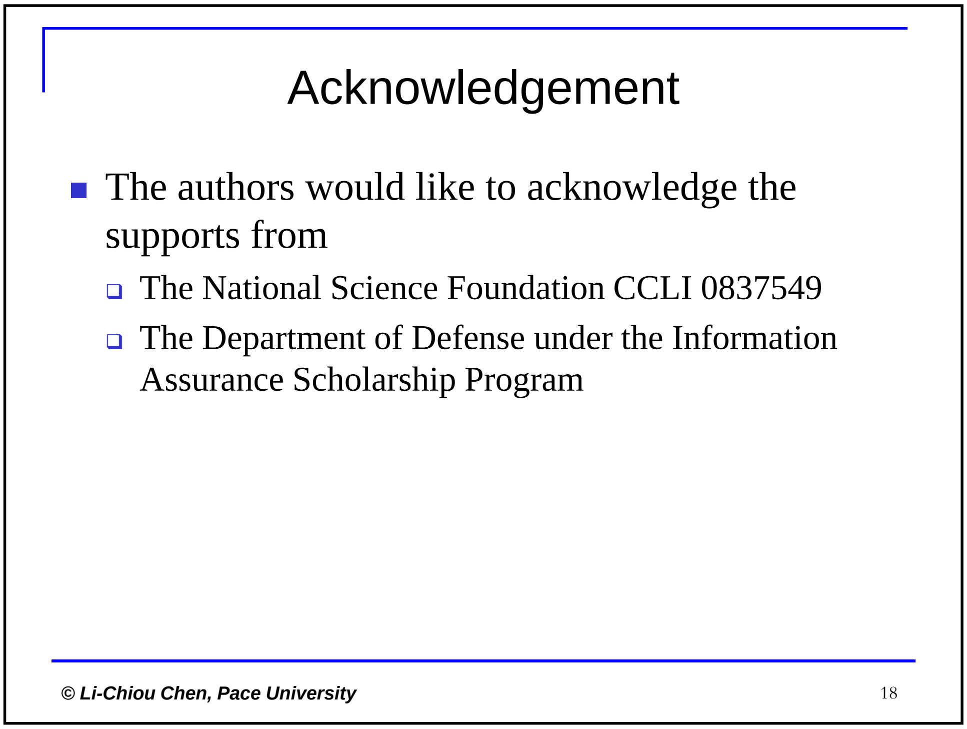
Project Evaluation: Questions

- **To what extent are the learning, teaching and laboratory materials developed and adapted?**
  - Quantitative: # of courses/students
  - Qualitative: lab observations, faculty interview
- **To what extent do the teaching modules & portable lab improve or enhance students' learning?**
  - Quantitative: standardized assessment & course evaluation
  - Qualitative: students' project reports & feedback
- **What is the impact of the project on facilitating the collaboration between faculty and industry partners?**
  - Quantitative: standardized survey instrument
  - Qualitative: interviews



Demo

- Example 1: web application overview
  - Ubuntu & Firefox
  - Observe HTTP commands
- Example 2: Web server vulnerability testing
  - Ubuntu, Firefox, Paros, Badstore.net web site
  - Crawl and Scan Badstore.net for vulnerabilities through a proxy server
- Example 3: Discover web vulnerability
  - OWASP Webgoat



Acknowledgement

- The authors would like to acknowledge the supports from
  - The National Science Foundation CCLI 0837549
  - The Department of Defense under the Information Assurance Scholarship Program