IERG 4130 Tutorial 1

The Chinese University of Hong Kong

Zirui Song

September 13, 2022

Outline

1. Course Arrangements
   - Tutorial
   - Office hour
2. Supplementary content
   - Authentication and Authorization
3. Assignments and Labs
   - Assignment Schedule
   - Lab introduction
   - Lab examples (SQL-injection, XSS)
4. Cyber Security in Daily Life

Websites

- Course website – https://course.ie.cuhk.edu.hk/ ierg4130/
  - For detailed teaching schedule
  - For course slides
- Piazza – https://piazza.com/cuhk.edu.hk/fall2022/ierg4130
  - Assignments and labs related
  - Exam arrangements related
  - Bonus!
  - ...

Tutorial

- Time slots
  - Tuesday 3:30pm – 4:15pm, MMW_710
  - Thursday 4:30pm – 5:15pm, LSK_410
- No attendance will be recorded
- Tutorial slides and recordings will be uploaded to Blackboard
- Important to help you with the assignments, labs and exams!

Office Hour

- Professor Zhang: Thursday 2:30pm – 3:30pm, or by appointment
  - Location: SHB 716
  - Make an appointment for other time slots via E-mail
- Tutors: 24/7 through the E-mail
  - Zirui Song: Thursday 3:30pm - 4:30pm
  - Ke Zhang: Wednesday 4:15pm - 5:15pm
  - Jiuqin Zhou: Monday 3:30pm - 4:30pm
  - Yikang Chen: Tuesday 4:15pm - 5:15pm
- Piazza: 24/7
  - Any one can discuss and answer the questions

Authentication and Authorization

- Authentication
  - Who you are
  - e.g., I am Alice/Bob
- Authorization
  - Whether you have privilege
  - e.g., I am an owner/guest

Authentication and Authorization

Authentication	Authorization
Authentication confirms your identity to grant access to the system.	Authorization determines whether you are authorized to access the resources.
It is the process of validating user credentials to gain user access.	It is the process of verifying whether access is allowed or not.
It determines whether user is what he claims to be.	It determines what user can and cannot access.
Authentication usually requires a username and a password.	Authentication factors required for authorization may vary, depending on the security level.
Authentication is the first step of authorization so always comes first.	Authorization is done after successful authentication.
For example, students of a particular university are required to authenticate themselves before accessing the student link of the university's official website. This is called authentication.	For example, authorization determines exactly what information the students are authorized to access on the university website after successful authentication.

Assignments and Labs

- Total 3 assignments = 30% of final score
  - Find hints in the lecture notes and tutorial slides
- Total 2 labs = 15% of final score
  - Offline, do it on your own computer
  - Try to launch some real-world attacks (funny!)
  - There will be tutorials to guide you and help you start

Assignments and Labs

- The Guideline is available in Blackboard

	Release Date	Topic	Due Date
Asg 1	Sep. 20	Software Security	Oct. 6
Lab 1	Sep. 20	Software Security	Oct. 27
Asg 2	Oct. 11	Cryptography	Oct. 27
Asg 3	Nov. 1	Network&Web Security	Nov. 22
Lab 2	Nov. 1	Network&Web Security	Dec. 1

Figure: The Arrangement of Assignments and Labs

Brief Introduction of the Lab

- Apply the learned theoretical knowledge to practical applications
  - In the lecture, you will learn the vulnerabilities of some applications
  - In the Lab, you are supposed to exploit the vulnerabilities and do attacks as a real hacker

- The Lab consists of two parts:
  - Software Security: Buffer-Overflow & Format String Vulnerability
  - Network & Web Security: TCP/IP Attack & XSS Attack

Lab Environment

- Environment setup: https://seedsecuritylabs.org/lab_env.html

Virtual Machine Software (VirtualBox)

① Install VirtualBox

Install the free VirtualBox. We recommend **Version 6.0.4** (please stay away from the newer versions, as they still have some issues with our VM). Although our instructions are only for VirtualBox, the pre-built VM images can also run on VMWare.

Pre-built Virtual Machine Images (Ubuntu)

All the SEED labs should be conducted in our pre-built virtual machine image, because we have installed all the necessary tools, software, and libraries that are needed by the SEED labs. Students just need to download the VM, and run it using VirtualBox (or VMWare).

- **SEED Ubuntu16.04 VM (32-bit)**: This VM was built in June 2019. We have made some small changes based on the 2018-May version.
  - Download the image from one of the following servers:
    - Google Drive: SEEDUbuntu-16.04-32bit.zip
    - DigitalOcean: SEEDUbuntu-16.04-32bit.zip
    - Cybersecurty.com: SEEDUbuntu-16.04-32bit.zip
    - Syracuse University (New York, US): SEEDUbuntu-16.04-32bit.zip
    - Zhejiang University (Zhejiang, China): SEEDUbuntu-16.04-32bit.zip
    - MD5 value: 12c48542c29c233580a23589b72b71b8

② Download SEED Ubuntu image, unzip

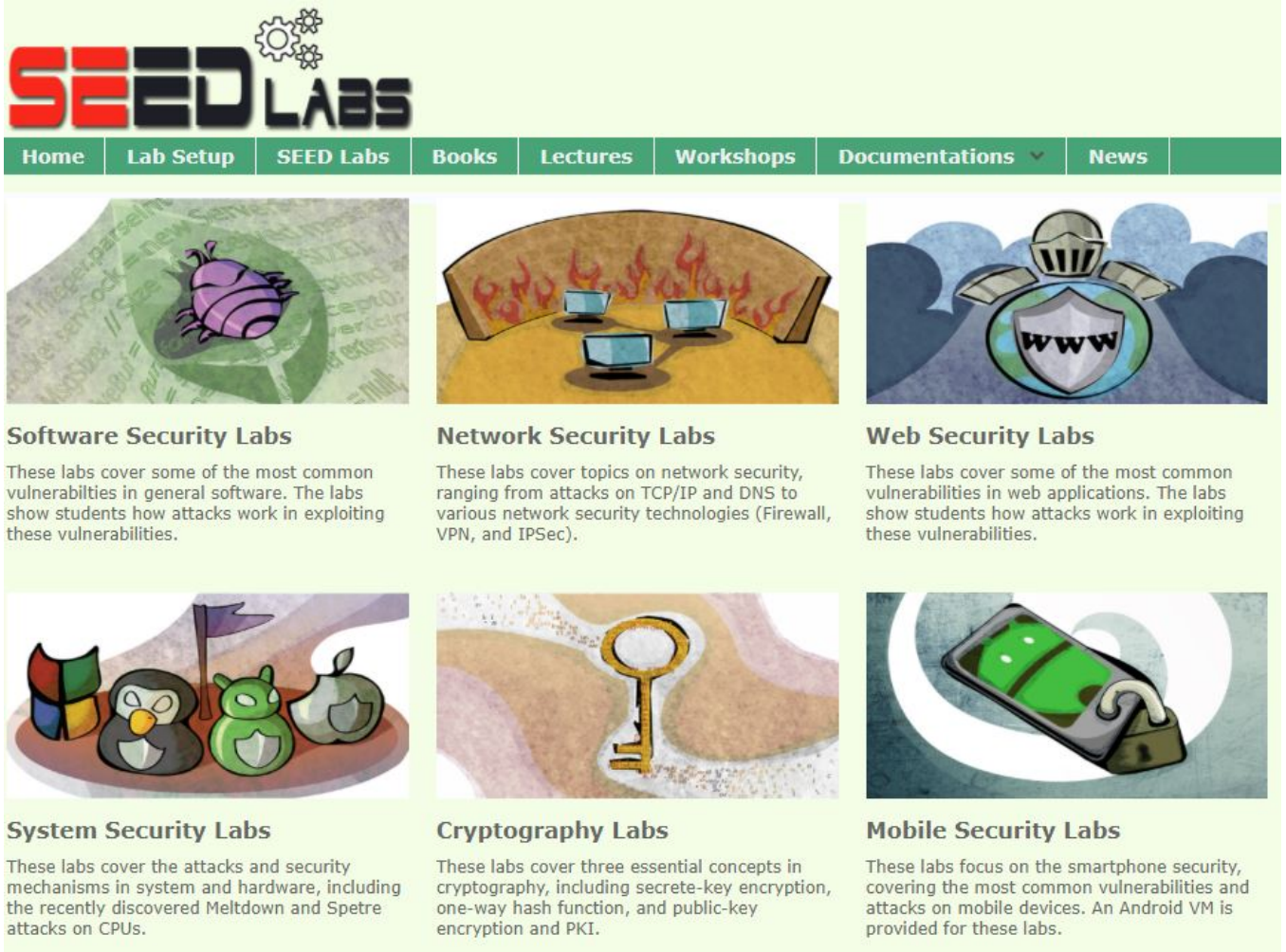
  - Unzip SEEDUbuntu-16.04-32bit.zip and you should be able to see a folder that contains the VM files.
    - Follow this document to run and configure the VM on VirtualBox.
    - You will be logged into an account called **seed**, and its password is **dees** (the reverse order of seed).

③ Configure Ubuntu

- **SEED Ubuntu12.04 VM (32-bit)**: This VM was built in Jaunary 2016; it has been phased out. However, two of the SEED labs still depend on this VM.
  - Download the image from the following server (the MD5 checksum of the file is 6ec9c429a2f4a9163530ada20f0621dc):
    - Main server
    - A server at Zhejiang University: SEEDUbuntu12.04.zip
  - User Manual: includes the account and password information, list of software and servers installed, and configuration.

Play by Yourself

- Lab Guideline: https://seedsecuritylabs.org/Labs_16.04/

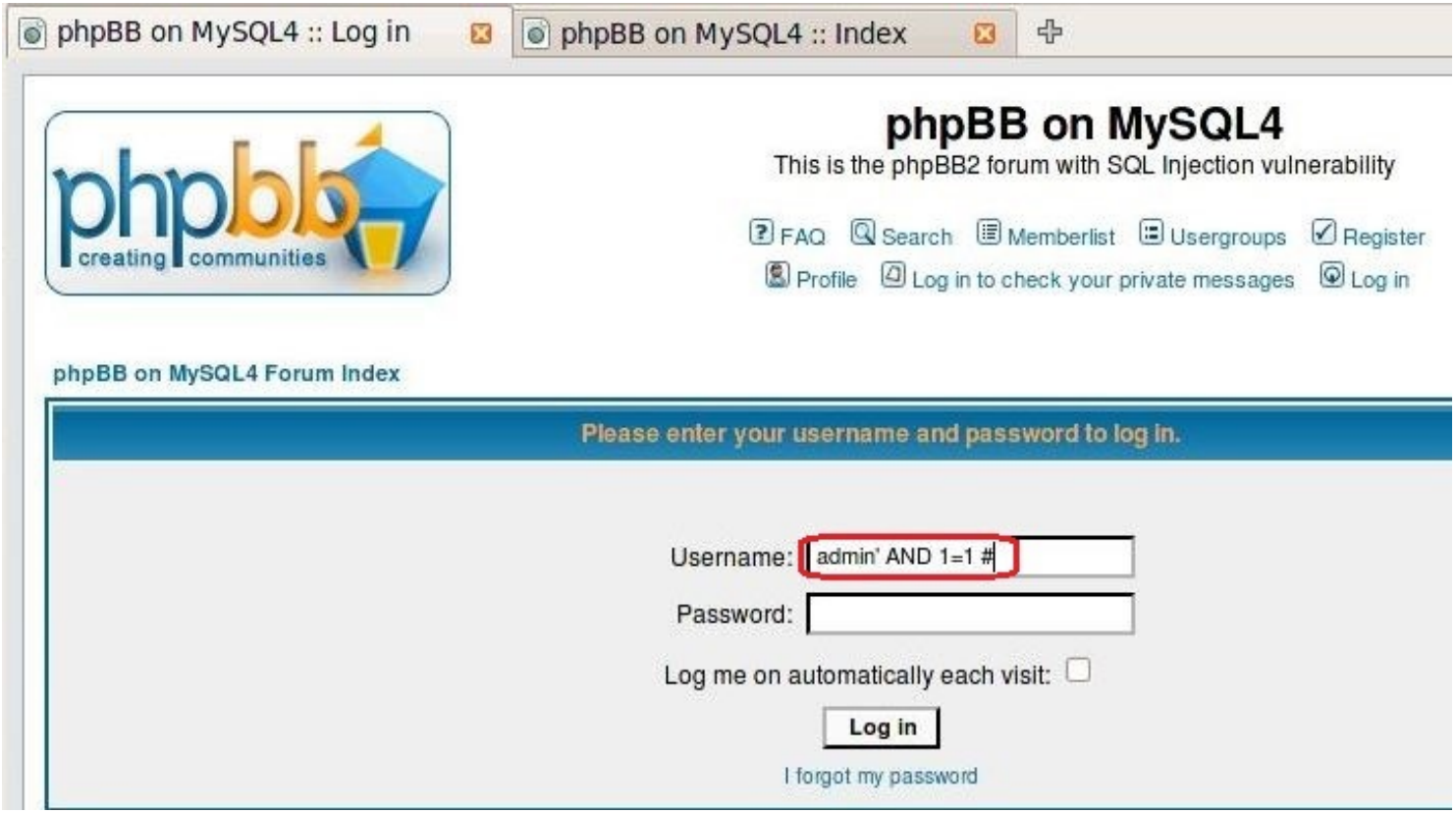


Linux Terminal Demo

- Demo: Terminal_demo.mp4
  - ls: list files
  - ping: use transport protocol to send out a response request message
  - CTRL+C: kill foreground process (i.e., terminate the current process)
  - cat: concatenate the file and print to the standard output device
  - gcc: compile the .c files into executable
  - ./[executable]: directly execute the executable files
  - ...

Lab Example: SQL Injection Attack

- Attacker can directly log in as the "Admin" without password



- Demo: SQL_injection.mp4

Lab Example

- Display an alert window by posting the message along with the JavaScript command

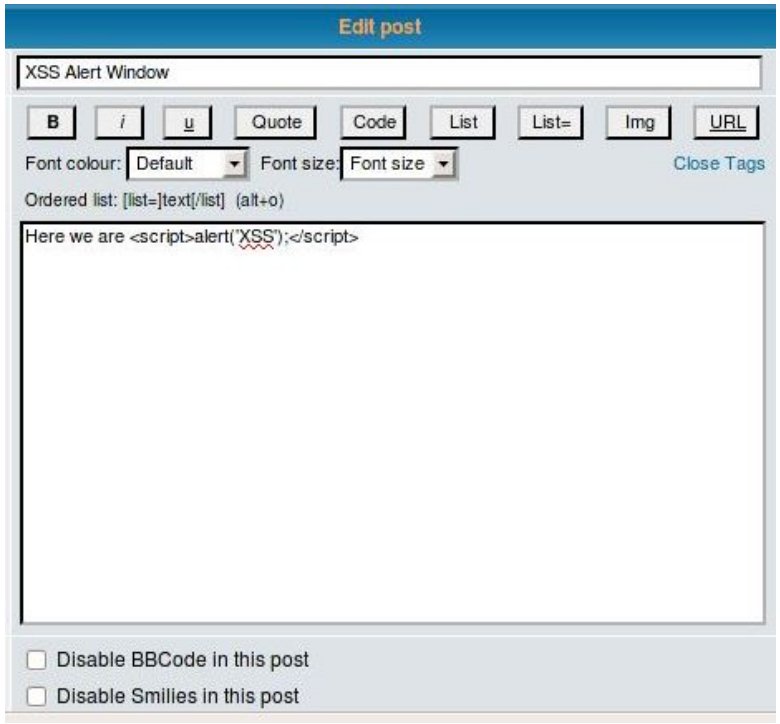


Figure: XSS Example

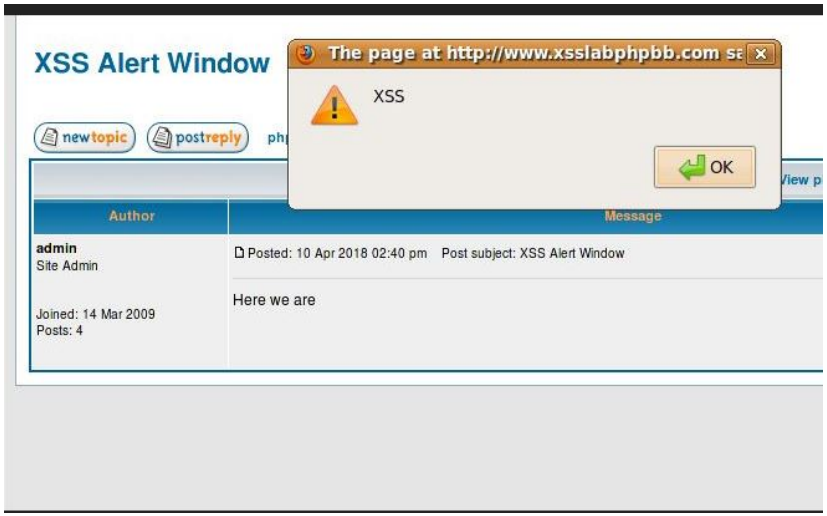


Figure: XSS Result

Cyber Security in Daily Life

- Stored XSS in the guide's GameplayVersion (www.dota2.com)
  - Reference: https://nosec.org/home/detail/2149.html