OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

6th Annual Cybersecurity Education Symposium

October 16, 2024

Programming with hacking: a hands-on approach to cyber-security education

Phu H. Phung

University of Dayton
Department of Computer Science

Marc Cahay

University of Cincinnati
Department of Electrical & Computer Engineering

About us - Marc Cahay

- BS/MS in Physics, PhD EE 1987
- Joint UC as Assistant Professor in 1989 (ECE Dept)
- Research: Nanoelectronics and Vacuum Electronics
- Head, Department of Electrical & Computer Engineering, University of Cincinnati, 2017-present
- Co-Director and Co-PI, Ohio Cyber Range Institute (with Hazem Said and Richard Harknett)
- Created new BS in Cybersecurity Engineering in ECE Department, Fall 2024 is 3rd year since inception, currently: 48 students, goal: 100 students by Fall of 2027.

About us - Phu H. Phung

- Associate Professor, Department of Computer Science, University of Dayton
- Visiting Scholar, Department of Electrical & Computer Engineering, University of Cincinnati
- Developed and the Point-of-Contact of UD’s BS in Computer Science with a concentration in Cyber Defense, designated as NSA NCAE-CD in 2022
- OCRI Cyber Educational Enhancement Fellow, 2024-2025, via SOCHE
- PI & Co-PI of multiple OCRI grants, via UD and SOCHE

Introduction to “Web Application Programming and Hacking,” a new course taught at UC

- Developed by Phu Phung, under Marc Cahay’s OCRI grant in Spring 2024
    - Hybrid in-person and asynchronous classes in Spring 2024
        - 128 students, including 3 undergraduates
    - Asynchronous classes in Summer 2024
        - 38 students with 3 graduates

Why should we combine programming with hacking?

- Most developers do not think like a hacker
    - “How could this be attacked?” [Credit: David A. Wheeler]
    - Without a hacker mindset, developers normally focus only on the functionalities
        - Programming books/courses do not teach how to develop secure software
            - Thus, software is vulnerable

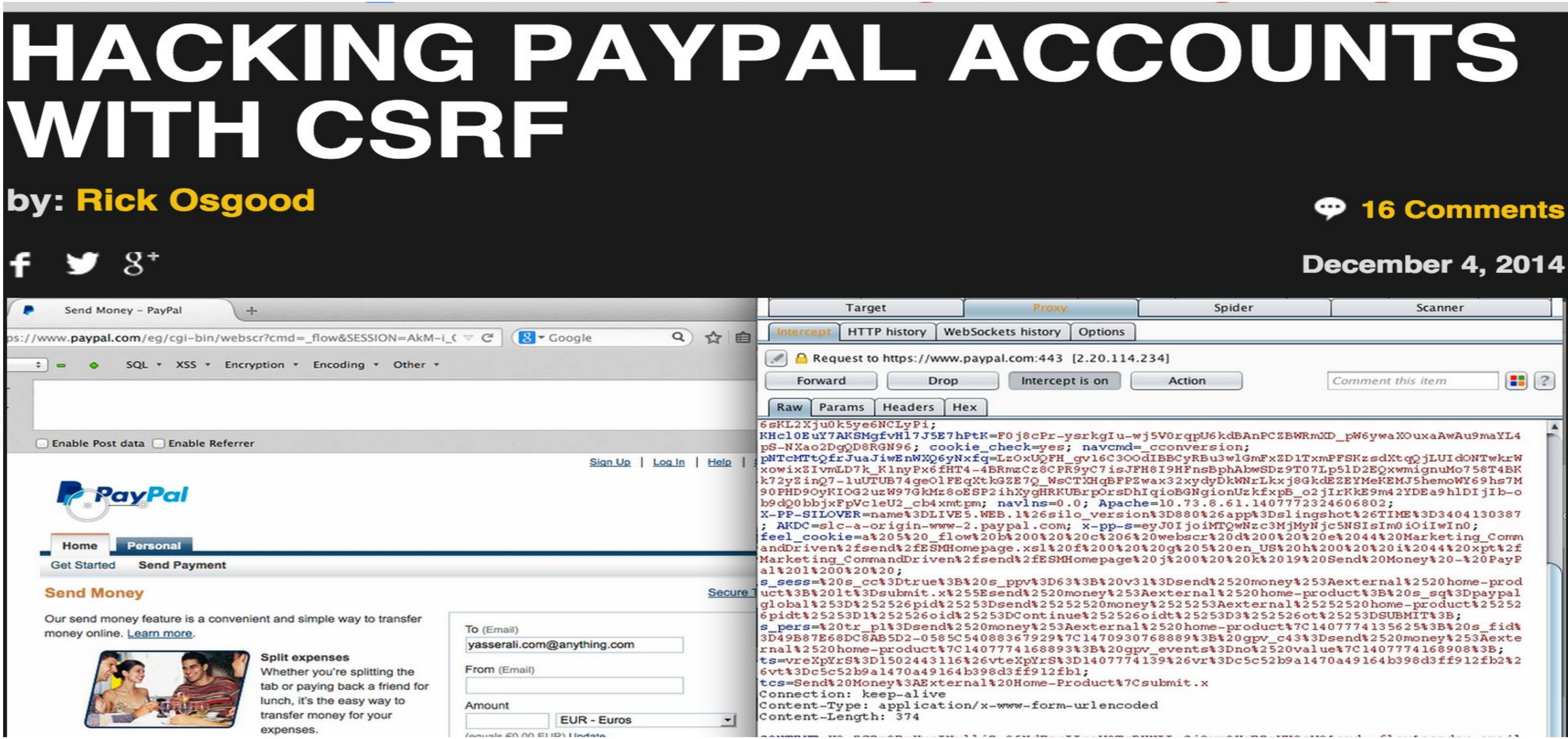
Lead to cyber attacks

A Real-world Attack Example

- Assume that you are a PayPal user, and assume that PayPal requires two-factor authentication, i.e., after providing username/password, you are required to confirm the login in another device
  - This mechanism prevents someone have your username/password to login to the system
- Discussion: is it safe for you to open a link like below while you are logged in to PayPal?

  https://www.paypal.com/eg/cgi-bin/cmd=flow&SESSION=Akl-tATMf1GOP-tQu3t3x4Vju&…

PayPal was vulnerable to CSRF



HACKING PAYPAL ACCOUNTS WITH CSRF

by: Rick Osgood

16 Comments

December 4, 2014

Send Money

Secure

Our send money feature is a convenient and simple way to transfer money online. Learn more.

Split expenses

Whether you're splitting the tab or paying back a friend for lunch, it's the easy way to transfer money for your expenses.

To (Email)
yasserali.com@anything.com

From (Email)

Amount
EUR - Euros

Request to https://www.paypal.com:443 [2.20.114.234]

```
6sKL2Xju0k5ye6NCLyPi;
KHcl0EuY7AKSMgfvHl7J5E7hPtK=F0j8cPr-ysrkgIu-wj5V0rqpU6kdBAnPCZBWRmXD_pW6ywaXOuxaAwAu9maYL4
pS-NXao2DgQD8RGN96; cookie_check=yes; navcmd=_cconversion;
pNTcMTtQfrJuaJiwEnWXQ6yNxfq=LzOxUQFH_gvl6C3OOdIBBCyRBu3wlGmFxZD1TxmPFSKzsdXtqQjLUIdONTwkrW
xowixZIvmLD7k_KlnyPx6fHT4-4BRmzCz8CPR9yC7isJFH8I9HFnsBphAbwSDz9T07Lp5lD2EQxwmignuMo758T4BK
k72yZinQ7-luUTUB74geOlFEqXtkGZE7Q_WsCTXHqBFPZwax32xydyDkWNrLkxj8GkdEZEYMeKEMJ5hemoWY69hs7M
90PHD9OyKIOG2uzW97GkMz8oESP2ihXygHRKUBrpOrsDhIqioBGNgionUzkfxpB_o2jIrKkE9m42YDEa9hlDIjIb-o
b9dQ0bbjxFpVcleU2_cb4xmtpm; navlns=0.0; Apache=10.73.8.61.1407772324606802;
X-PP-SILOVER=name%3DLIVE5.WEB.1%26silo_version%3D880%26app%3Dslingshot%26TIME%3D3404130387
; AKDC=slc-a-origin-www-2.paypal.com; x-pp-s=eyJ0IjoiMTQwNzc3MjMyNjc5NSIsIm0iOiIwIn0;
feel_cookie=a%205%20_flow%20b%200%20%20c%206%20webscr%20d%200%20%20e%2044%20Marketing_Comm
andDriven%2fsend%2fESMHomepage.xsl%20f%200%20%20g%205%20en_US%20h%200%20%20i%2044%20xpt%2f
Marketing_CommandDriven%2fsend%2fESMHomepage%20j%200%20%20k%2019%20Send%20Money%20-%20PayP
al%201%200%20%20;
s_sess=%20s_cc%3Dtrue%3B%20s_ppv%3D63%3B%20v31%3Dsend%2520money%253Aexternal%2520home-prod
uct%3B%20lt%3Dsubmit.x%255Esend%2520money%253Aexternal%2520home-product%3B%20s_sq%3Dpaypal
global%253D%252526pid%25253Dsend%2525252520money%2525253Aexternal%25252520home-product%25252
6pidt%25253D1%252526oid%25253DContinue%252526oidt%25253D3%252526ot%25253DSUBMIT%3B;
s_pers=%20tr_pl%3Dsend%2520money%253Aexternal%2520home-product%7C1407774135625%3B%20s_fid%
3D49B87E68DC8AB5D2-0585C54088367929%7C1470930768889%3B%20gpv_c43%3Dsend%2520money%253Aexte
rnal%2520home-product%7C1407774168893%3B%20gpv_events%3Dno%2520value%7C1407774168908%3B;
ts=vreXpYrS%3D1502443116%26vteXpYrS%3D1407774139%26vr%3Dc5c52b9a1470a49164b398d3ff912fb2%2
6vt%3Dc5c52b9a1470a49164b398d3ff912fbl;
tcs=Send%20Money%3AExternal%20Home-Product%7Csubmit.x
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 374
```

Who should be responsible for the PayPal attack example?

- The user?
  - e.g., using anti-virus software, or cybersecurity awareness?
- The user's organization?
  - E.g., using a proxy filtering, firewalls?
- The Internet Provider?
  - e.g., installing firewalls?

Conventional Security Solutions such as anti-virus software or firewall cannot prevent attacks caused by software vulnerabilities

Why does an CSRF attack (like in PayPal) happen?

- An CSRF (cross-site request forgery) attack might happen due to:
  - The code, i.e., the developer, assumes that the request was initiated by the authenticated user
    - (the request actually came from an active session in the same browser)
    - No further verification
- Revisit: Most developers do not think like a hacker
  - "How could this be attacked?"

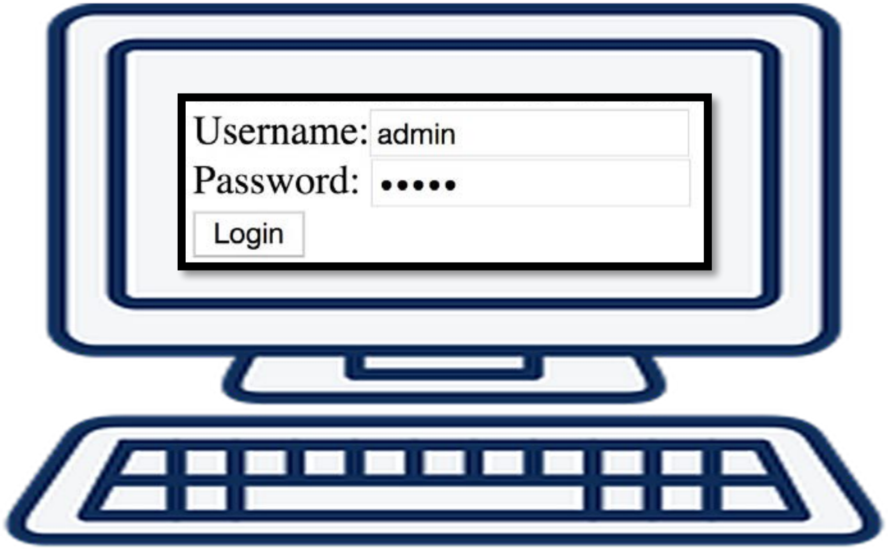
Real-world hacking experiences will help developers to understand and avoid/prevent the issues

Web Application Programming and Hacking (WAPH) – Course overview

- Study basic web application development with front-end (HTML5, JavaScript, CSS) and back-end (PHP/MySQL).
- Web application vulnerabilities and attacks will be introduced and explored with hands-on exercises on the range.
  - Secure programming principles and practices will be introduced to avoid potential web application vulnerabilities and attacks.
- A project-based course to apply the learned concepts to develop and deploy a real-world application to the Cloud, from front-end to back-end and database, through
  - Practical hands-on programming labs
  - Hackathons (hacking exercises)
  - Individual projects
  - A team project

A programming exercise example (WAPH-Lab3.b)

- Checking login credentials:



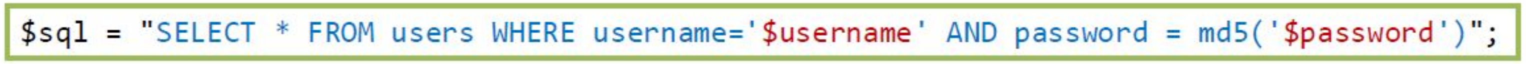
Username: admin

Password: •••••

# a simple/simplified algorithm

1. get the input data (username/password)

2. Construct a SQL query from the input to compare with the data in the database, i.e.:

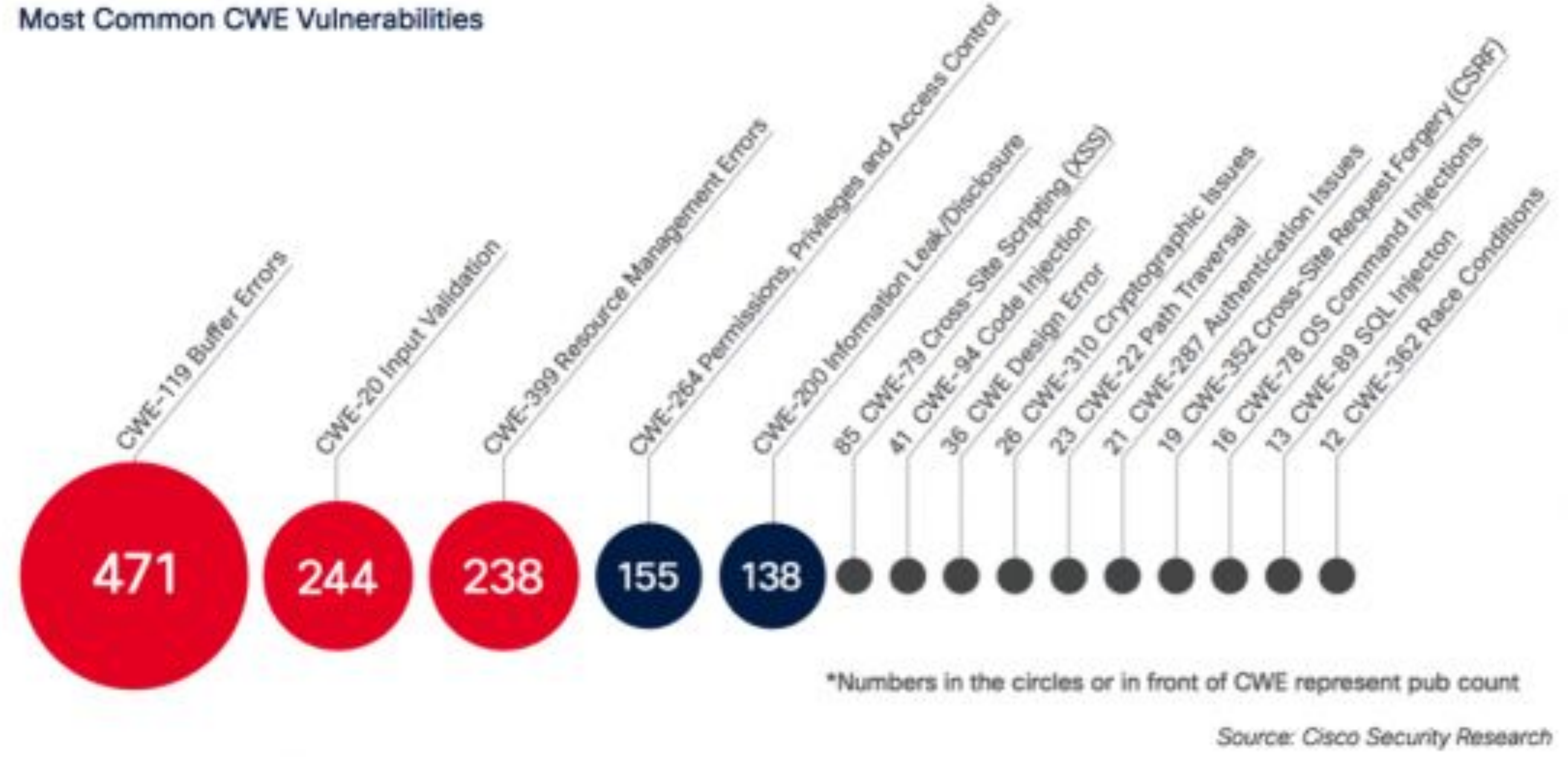


```
$sql = "SELECT * FROM users WHERE username='$username' AND password = md5('$password')";
```

3. return TRUE/FALSE

Coding + Testing => DONE

Common Software Vulnerabilities



Most Common CWE Vulnerabilities

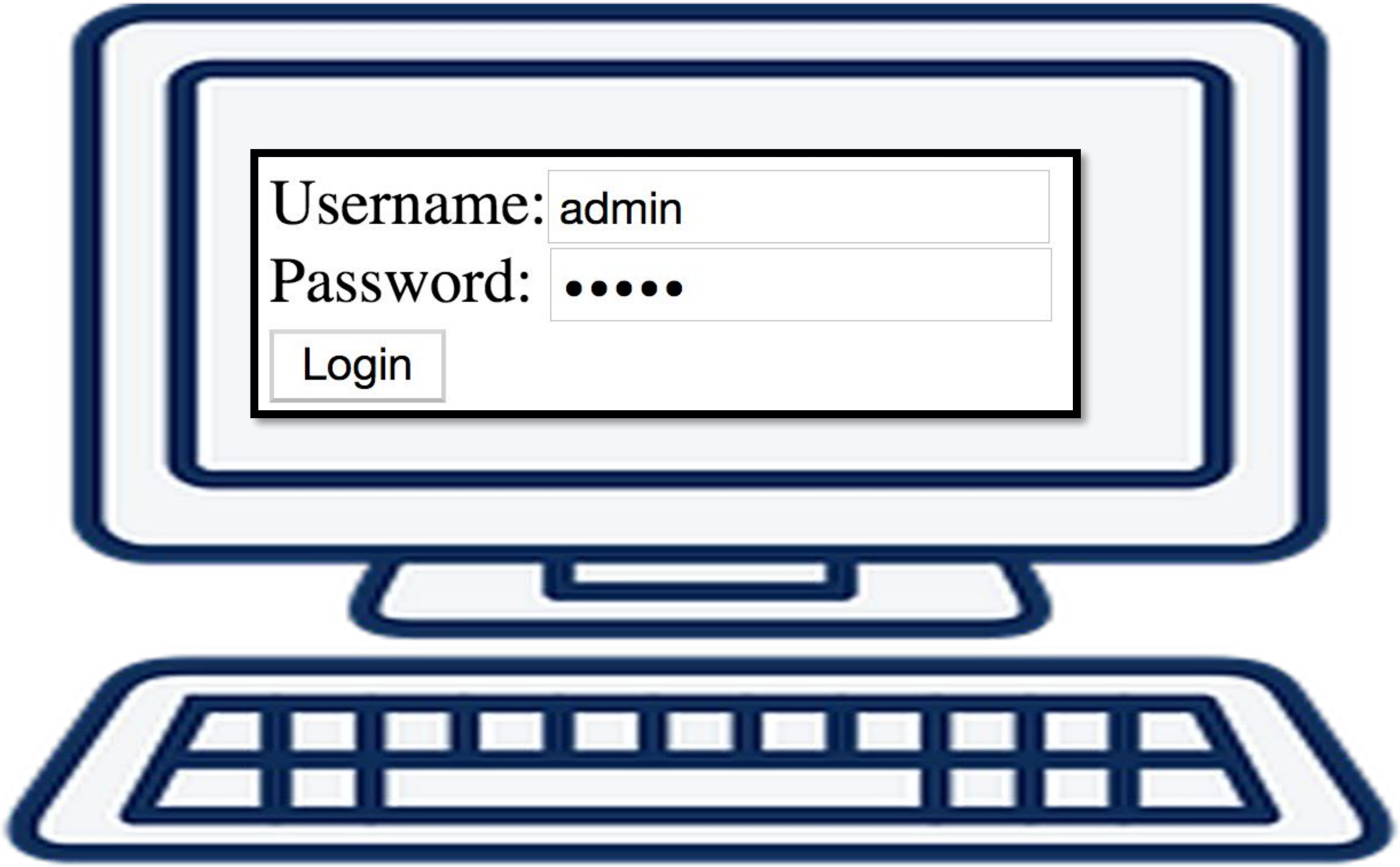
*Numbers in the circles or in front of CWE represent pub count

Source: Cisco Security Research

The most common programming mistake

- No input validation
    - Example - checking login credentials: do not validate the input data before using it
        - What could go wrong?
            - Without a hacker mindset and real hacking experiences, developers might not understand the consequences of vulnerabilities,
                - Not applying secure programming techniques

A hacking exercise example
WAPH-Hackathon-2: SQL Injection Attacks & Defenses



Username: admin

Password: •••••

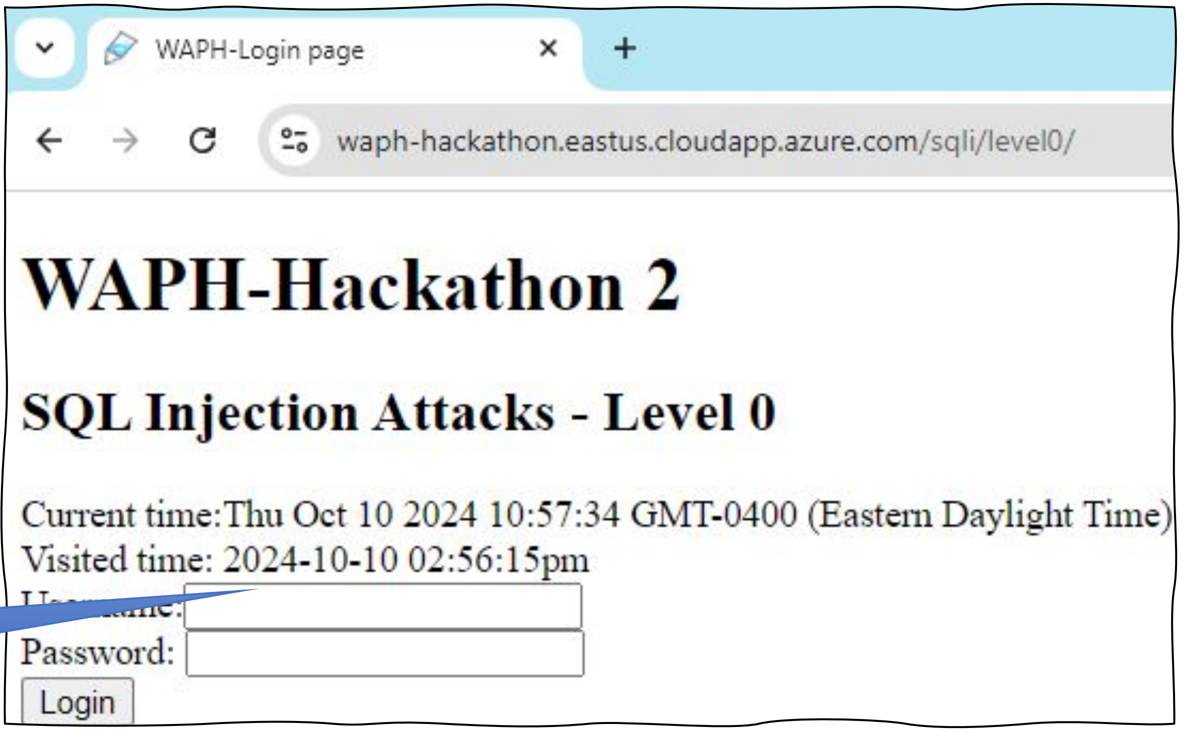
Pretend as a hacker, students would learn how to inject SQL code from input to bypass a vulnerable SQL-based authentication system

WAPH-Hackathon-2-Level-0: SQL Injection hacking exercise example

Live hacking & demo: https://bit.ly/waph-sqli0 -> https://waph-hackathon.eastus.cloudapp.azure.com/sqli/level0/

Students’ task: ***Inject SQL code with their University’s username to bypass the login check and successfully log in to the system.***

```
phungph' OR 1=1#
```



WAPH-Hackathon 2

SQL Injection Attacks - Level 0

Current time:Thu Oct 10 2024 10:57:34 GMT-0400 (Eastern Daylight Time)
Visited time: 2024-10-10 02:56:15pm

Username:
Password:
Login

WAPH-Hackathon-2-Level-1:
SQL Injection hacking exercise example

Live hacking & demo:
https://waph-hackathon.eastus.cloudapp.azure.com/sqli/level1/

Solution from Level 0 would not work.

Students' task: ***Guess the code in the back-end & inject SQL code with their University's username to bypass the login check and successfully log in to the system.***

```
phungph" OR 1=1 limit 1#
```

WAPH-Hackathon-2-Level-2: SQL Injection hacking exercise example

Live hacking & demo:
https://waph-hackathon.eastus.cloudapp.azure.com/sqli/level2/

The login system is completely protected from to SQLi attacks (students will learn how to implement this in Lab 3.d); however, there is another "back-door" in the system vulnerable to SQLi attacks.

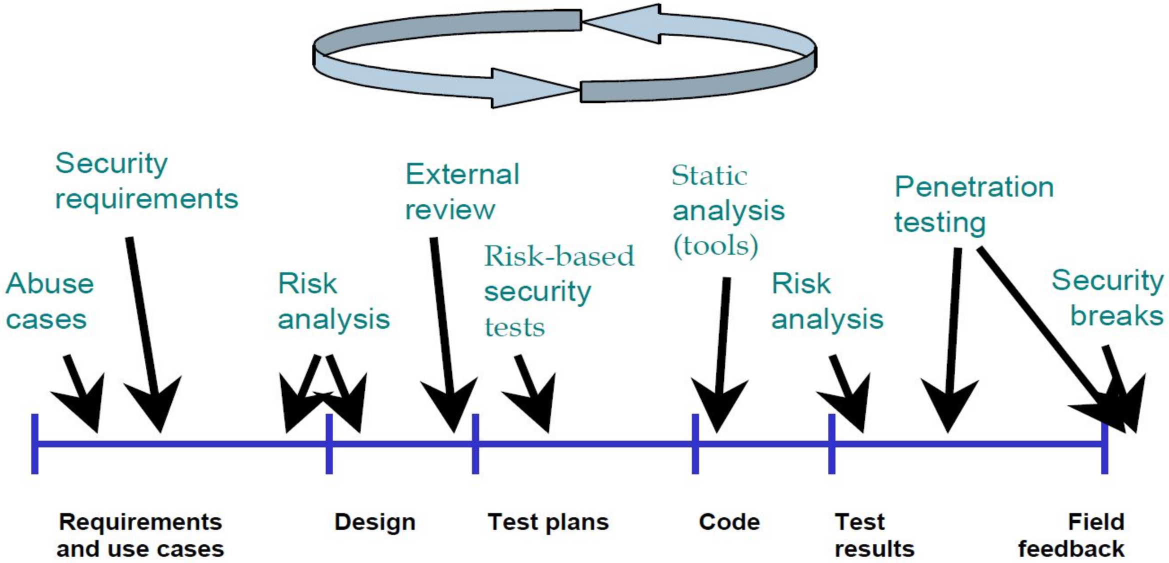
Students' task: ***Discover the vulnerability, using SQLi attacks to steal usernames/passwords from the database to log in to the system.***

Hacking is not to attack

- Hacking techniques help to
  - understand the security system engineering, programming weaknesses and their consequences, e.g.,: CSRF in PayPal, SQLi, and other attacks
    - Apply secure programming techniques
      - defend against the possible vulnerabilities
  - design secure systems and write secure code

Secure Programming: Security at the source

- Secure Development Lifecycle
  - The developers should be responsible for security at the design and development phase



Source: "Improving Security Across the Software Development Lifecycle – Task Force Report", April 1, 2004. http://www.cyberpartnership.org/init.html; based on Gary McGraw 2004, IEEE Security and Privacy.

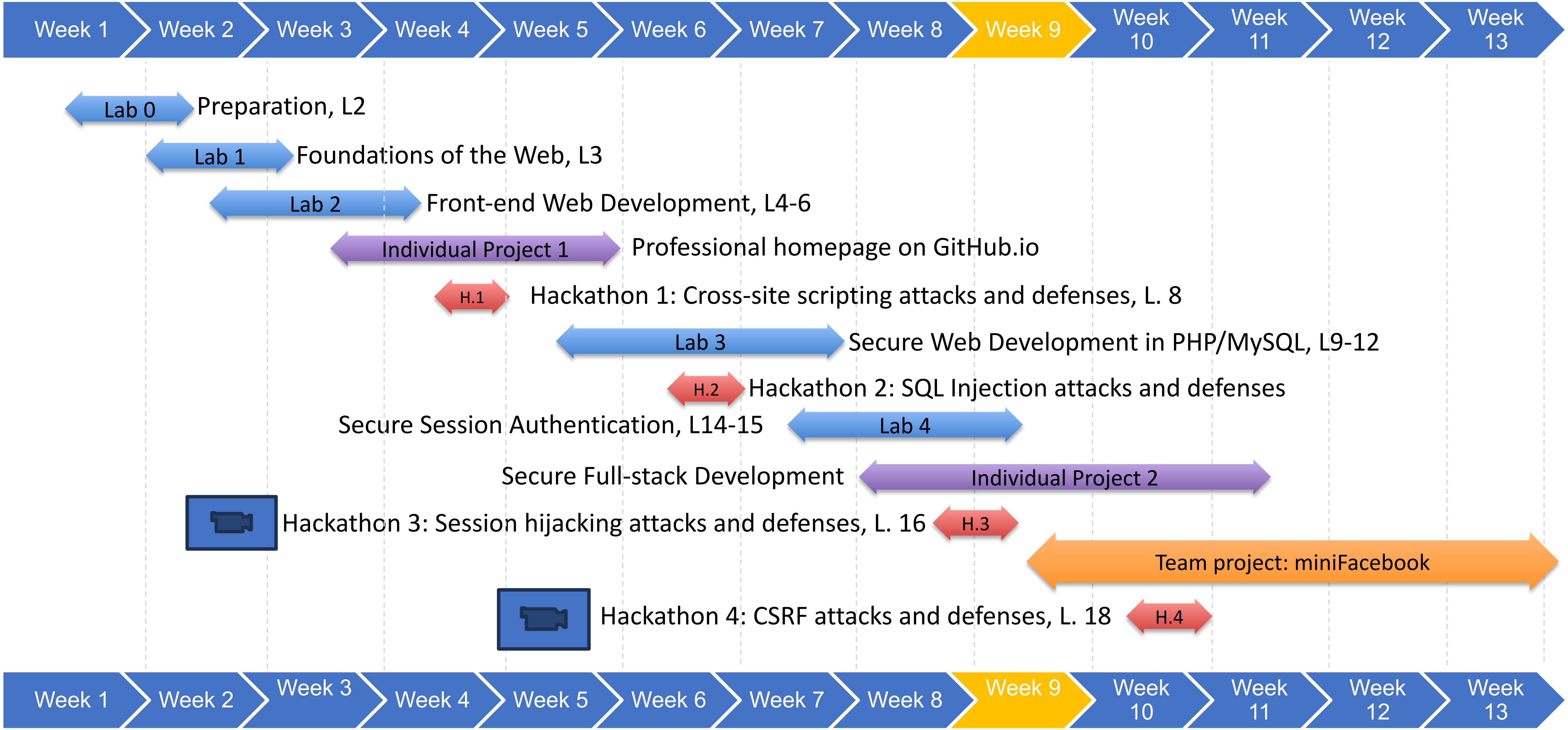
Secure Programming Example (WAPH-Lab3.d)

OWASP Primary Defenses against SQL Injection Attacks:
Option #1: Use of Prepared Statements

- Prepared Statement Implementation
  - Steps provided to implement Prepared Statements in PHP/MySQL
- **Security Analysis**
  - **Prepared Statement Explanation**: Discuss why prepared statements can prevent SQL injection attacks
  - **Discussions**: Are there any programming flaws/vulnerabilities in the current code?

Web Application Programming and Hacking (WAPH)

Course roadmap with 12.5-week schedule



Week 1 | Week 2 | Week 3 | Week 4 | Week 5 | Week 6 | Week 7 | Week 8 | Week 9 | Week 10 | Week 11 | Week 12 | Week 13

Lab 0 Preparation, L2

Lab 1 Foundations of the Web, L3

Lab 2 Front-end Web Development, L4-6

Individual Project 1 Professional homepage on GitHub.io

H.1 Hackathon 1: Cross-site scripting attacks and defenses, L. 8

Lab 3 Secure Web Development in PHP/MySQL, L9-12

H.2 Hackathon 2: SQL Injection attacks and defenses

Secure Session Authentication, L14-15 Lab 4

Secure Full-stack Development Individual Project 2

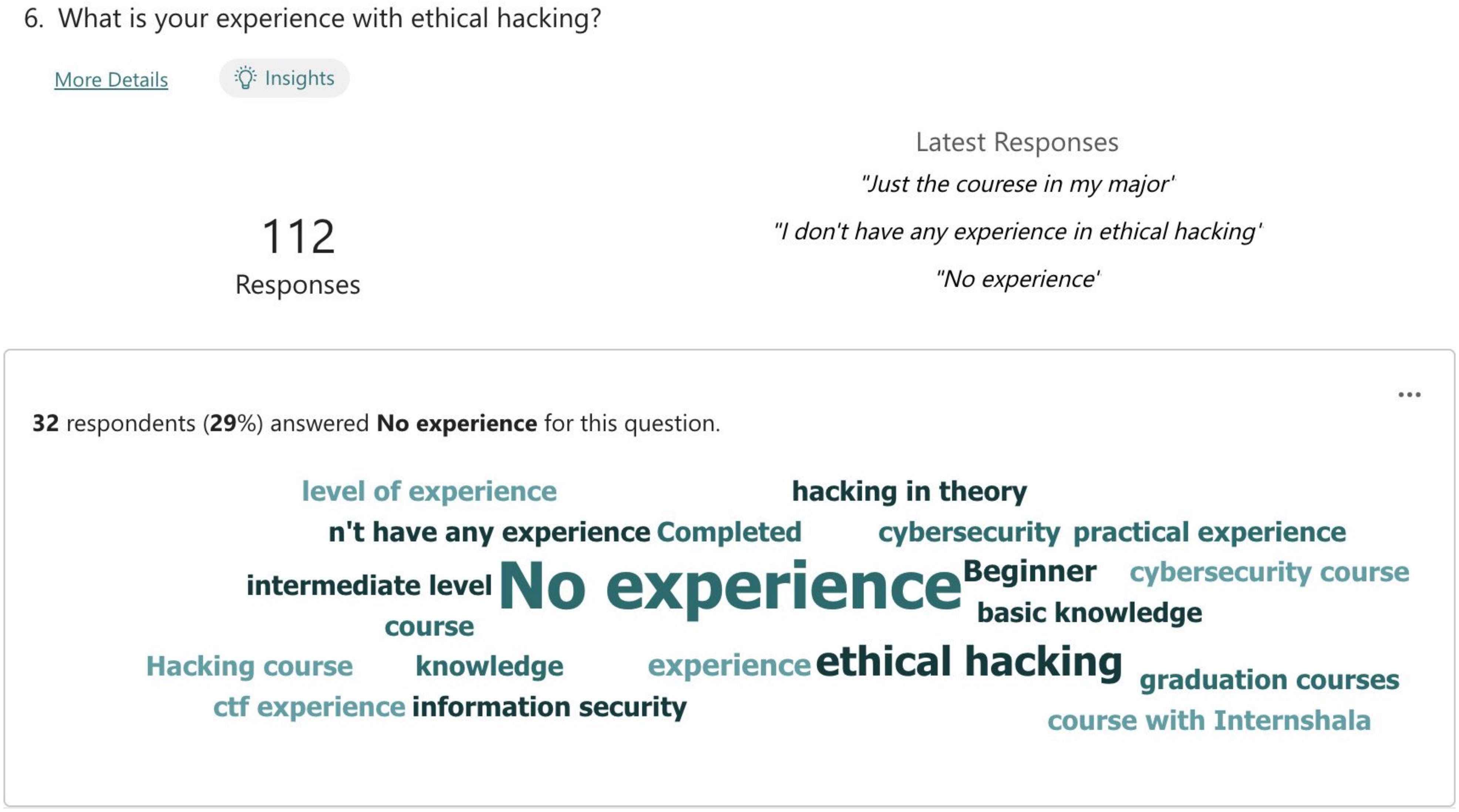
Hackathon 3: Session hijacking attacks and defenses, L. 16 H.3

Team project: miniFacebook

Hackathon 4: CSRF attacks and defenses, L. 18 H.4

Week 1 | Week 2 | Week 3 | Week 4 | Week 5 | Week 6 | Week 7 | Week 8 | Week 9 | Week 10 | Week 11 | Week 12 | Week 13

Web Application Programming and Hacking (WAPH) Students’ experience pre-class survey



6. What is your experience with ethical hacking?

112

Responses

Latest Responses

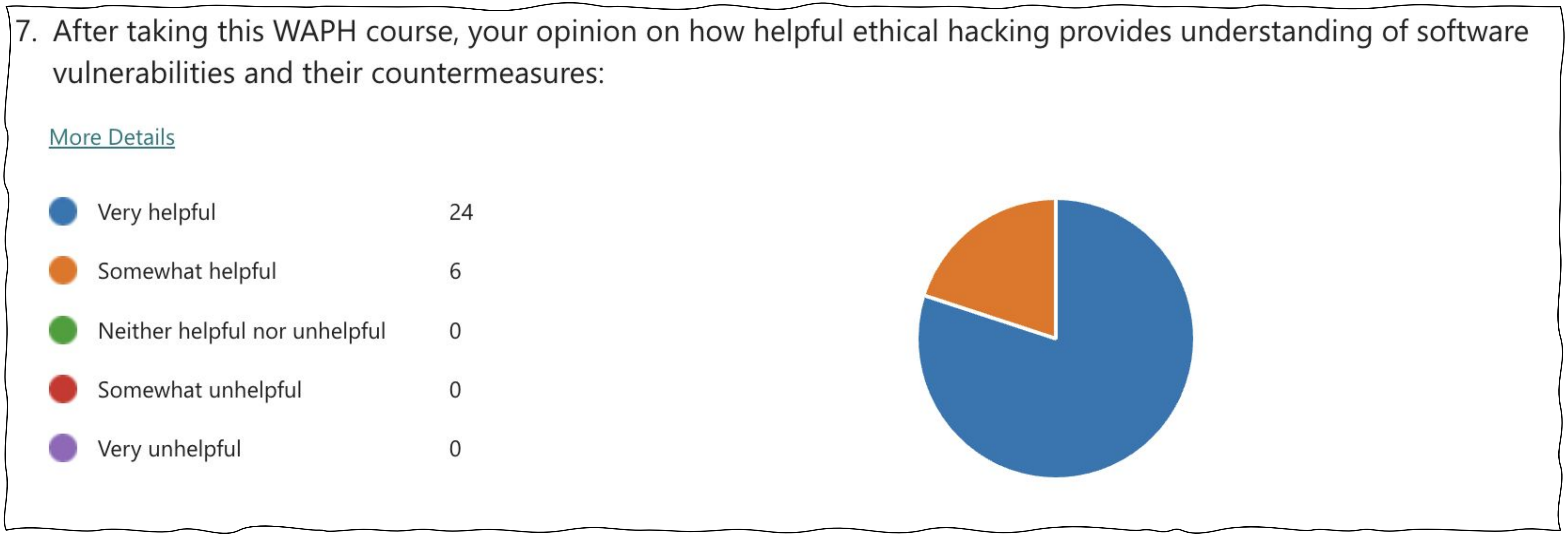
"Just the courese in my major"

"I don't have any experience in ethical hacking"

"No experience"

32 respondents (**29**%) answered **No experience** for this question.

Web Application Programming and Hacking (WAPH) Students’ experience post-class survey



7. After taking this WAPH course, your opinion on how helpful ethical hacking provides understanding of software vulnerabilities and their countermeasures:

More Details

🔵	Very helpful	24
🟠	Somewhat helpful	6
🟢	Neither helpful nor unhelpful	0
🔴	Somewhat unhelpful	0
🟣	Very unhelpful	0

Full survey ->

Students’ feedback

“This is the best course i’ve taken on software development that included security. …”

“As a cybersecurity engineering major this course was just perfect. I learned so many important basic cybersecurity skills that I feel I should have been taught sooner. …”

“… I particularly liked the engaging assignments, hackathons, and projects, all thoughtfully designed to provide practical experience aligned with the course material. …”

Ethical Hacking Labs’ Environments

- The code has been developed by the instructor, and deployed on a virtual environment
  - Option 1: Vulnerable applications/servers deployed on a cyber range, e.g., OCRI Cyber Range
    - Need IT setup, not scale well with large number of students
  - Option 2: Vulnerable applications/servers deployed on the Cloud, e.g., https://waph-hackathon.eastus.cloudapp.azure.com
    - Code and plug-n-play setup are available

Discussions

A security engineering student's comment: *"…I'm surprised this course is not taught full time and required for cybersecurity students. …"*

- Hacking techniques and security courses are important!
  - Combing programming with hacking, like *Web Application Programming and Hacking,* has demonstrated significant impact on security awareness for developers
- However, security courses are not mandatory for CS/CE/IT students
  - Future developers still write insecure code !!!
    - Software vulnerabilities are rising

Future development

- Currently developing hacking labs to be available on the OCRI Cyber Library
- Integrate security/hacking mini-modules in programming classes
- Collaborate with other institutions to explore the possibilities to integrate security/hacking components in their curricula