CS 370
Introduction to Security

Course Intro

Instructor: Yeongjin Jang

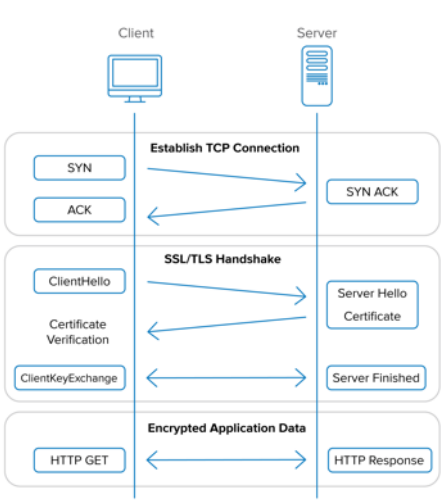
- At OSU Since Oct 2017
- Main research area: systems security
- Hacking
  - CPU side-channel attacks, Jailbreaking, exploit development, automatic hacking (fuzzing / symbolic execution), designing secure systems, software security, blockchain, DeFi, etc..
- Faculty advisor of OSUSEC
- CS444/544 Operating Systems II
- CS499/579 Cyber Attacks and Defense
- CS499/579 Systems Security
- Feel free to reach me if you are interested in cybersecurity…
  - Join OSUSEC!

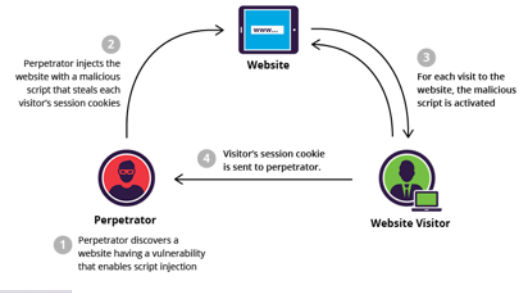
Course Description

- Goal: Learn modern cybersecurity techniques
- Target: **Beginners**

- **Lecture** & **Micro-assignments**
  - Learn *high-level fundamental concepts* in the lecture
  - *Practice engineering details* with micro-assignments
  - There will be many assignments, but they are small and fun

- Topics
  - Cryptography (Symmetric, Asymmetric, HMAC)
  - Network Security (SSL/TLS and PKI)
  - Authentication (Password/Private Key/Biometrics/Multi-factor)
  - Web Security (SQLi, parameter injection, XSS, CSRF, etc.)
  - Software Security (Buffer overflow, logic bugs, static and dynamic analysis)
  - Malware, Phishing, Ransomware, Privacy, and others..





Course Objective

- Learn modern security technologies
- Be able to answer the following questions:
  - How and why can **cryptography make our communication secure?**
  - How can we **ensure the other end at online is the right entity** (person/server)?
  - Why should we use **two- or multi-factor authentication**? What makes **attackers difficult** for doing what?
  - What are the **effect of incorrectly deployed systems** (Web/Software)?
    - How does **hacking work**? What can **attackers do**?
  - What is malware, and why are they dangerous?
  - How can the **Stuxnet malware break Iranian Nuclear Facility remotely**?
  - Why **can't we decrypt ransomware encrypted files**?
    - Why **can we decrypt for some other ransomware**?

Important Links

- Website: https://cs370.unexploitable.systems/
- Instructor: Dr. Yeongjin Jang (yeongjin.jang@oregonstate.edu)
- TAs:
  - Jeevan John
- Scoring Server: https://ctf.unexploitable.systems
- Discord Server: https://discord.gg/KbnnWNCr2k
- Assignment server: vm-ctf1.eecs.oregonstate.edu
  - Please connect this via flip
  - Instructions: https://cs370.unexploitable.systems/rules.html

Course Structure

- 10 weeks schedule
  - https://cs370.unexploitable.systems/cal.html
  - Cryptography (2 weeks)
  - Network Security (2 weeks)
  - Authentication (1 week)
  - Web security (1 week)
  - Software security (1 week)
  - Malware and others (1 week)
  - NSA Codebreaker (1 week)
  - Quizzes (1 week)

Tuesday	Wednesday	Thursday
Sep 20	Sep 21	Sep 22 **LEC 1:** Course Introduction **Preparation:** Finish Registration *First day of class*
Sep 27 **LEC 2:** Ancient Cryptography and Cryptography Basics	Sep 28	Sep 29 **LEC 3:** Symmetric Encryption (DES/AES)
Oct 4 **LEC 4:** Asymmetric Encryption, Key Exchange Algorithms, and Digital Signatures (RSA & Diffie--Hellman)	Oct 5	Oct 6 **LEC 5:** Cryptographic Hash (MD5/SHA1--3) and Message Authentication Code (MAC)
Oct 11 **LEC 6:** Secure Socket Layer (SSL) and Transportation Layer Security (TLS) **DUE:** Cryptography challenges	Oct 12	Oct 13 **LEC 7:** Public-key Infrastructure (PKI), Digital Certificates, and HTTPS
Oct 18 **LEC 8:** Quiz 1 prep (cryptography and network security)	Oct 19	Oct 20 Quiz 1 (Cryptography and Network Security)
Oct 25 **LEC 9:** User Authentication (password/public-key) **DUE:** SSL/TLS and PKI challenges	Oct 26	Oct 27 **LEC 10:** Multi-factor and Biometric Authentications
Nov 1 **LEC 11:** Web Security Basics (Parameter/SQL injection & directory listing)	Nov 2	Nov 3 **LEC 12:** Advanced Web Security (XSS, CSRF, etc.)
Nov 8 **LEC 13:** Codebreaker Prep 1 (network security) **DUE:** Authentication and Web Security challenges	Nov 9	Nov 10 **LEC 14:** Codebreaker Prep 2 (web/software security)
Nov 15 **LEC 15:** Software Vulnerabilities (Buffer overflow, Logic bugs, etc.)	Nov 16	Nov 17 **LEC 16:** Static and Dynamic analysis (CodeQL & Fuzzing)

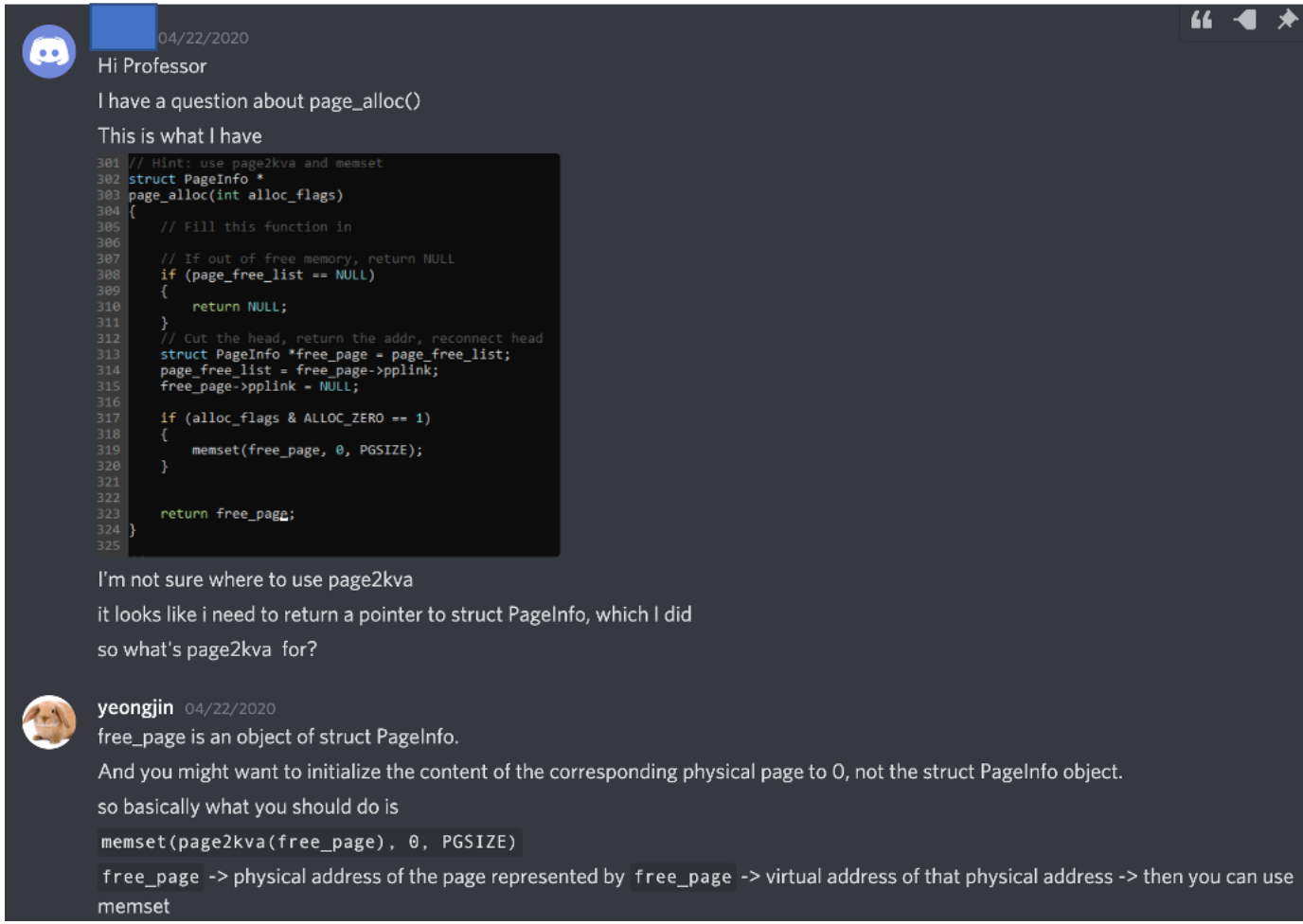
- In-person (Zoom sync) lectures (videos will be available on YouTube)
- TA/myself address questions on Discord

Meeting Time (with me)

- Lecture (in-person, video, **synchronous**)
  - Tu/Th 2:00pm
  - Video link will be available on Canvas/Homepage after 6 pm
  - Synchronous Zoom link:
    - https://oregonstate.zoom.us/j/97364167540?pwd=S3B6dFowSjZGNU44M1g4aFQrc2kyQT09
- My office hour (@ KEC 3079)
  - Wed 05:30pm – 07:00pm

TA Office Hours

- Availability will be posted later…
- Ask any questions
- Please help each other
- Discord Server
  - https://discord.gg/KbnnWNCr2k



Grading (Can be changed)

- 60% micro assignments
  - 15% each per assignment set
- 20% Quizzes (mini-exam)
  - Quiz 1 (10/20) : Cryptography and Network Security
  - Quiz 2 (11/22): Authentication and Web/Software Security

- All quizzes will be on CANVAS (remote)
  - Fully open material (do not search on the Internet)
  - You will have up to 3 trials (I will take your best score)
  - ~60 minutes at most, but I will set the time as 120min

Micro-Assignments (60%)

- Four sets
  - Set 1: Cryptography challenges
    - Practice **how to encrypt data**
    - Practice **how to break** crypto schemes
    - Play with **digital signatures**
    - Practice **what can go wrong** if there is **no message authentication**
  - Set 2: SSL/TLS and PKI
    - Practice **how SSL/TLS works**
    - Practice **how certificates are utilized in authentication**
    - Know **how to construct secure communication channel**
    - Know **how to attack such constructions…**

Micro-Assignments (60%)

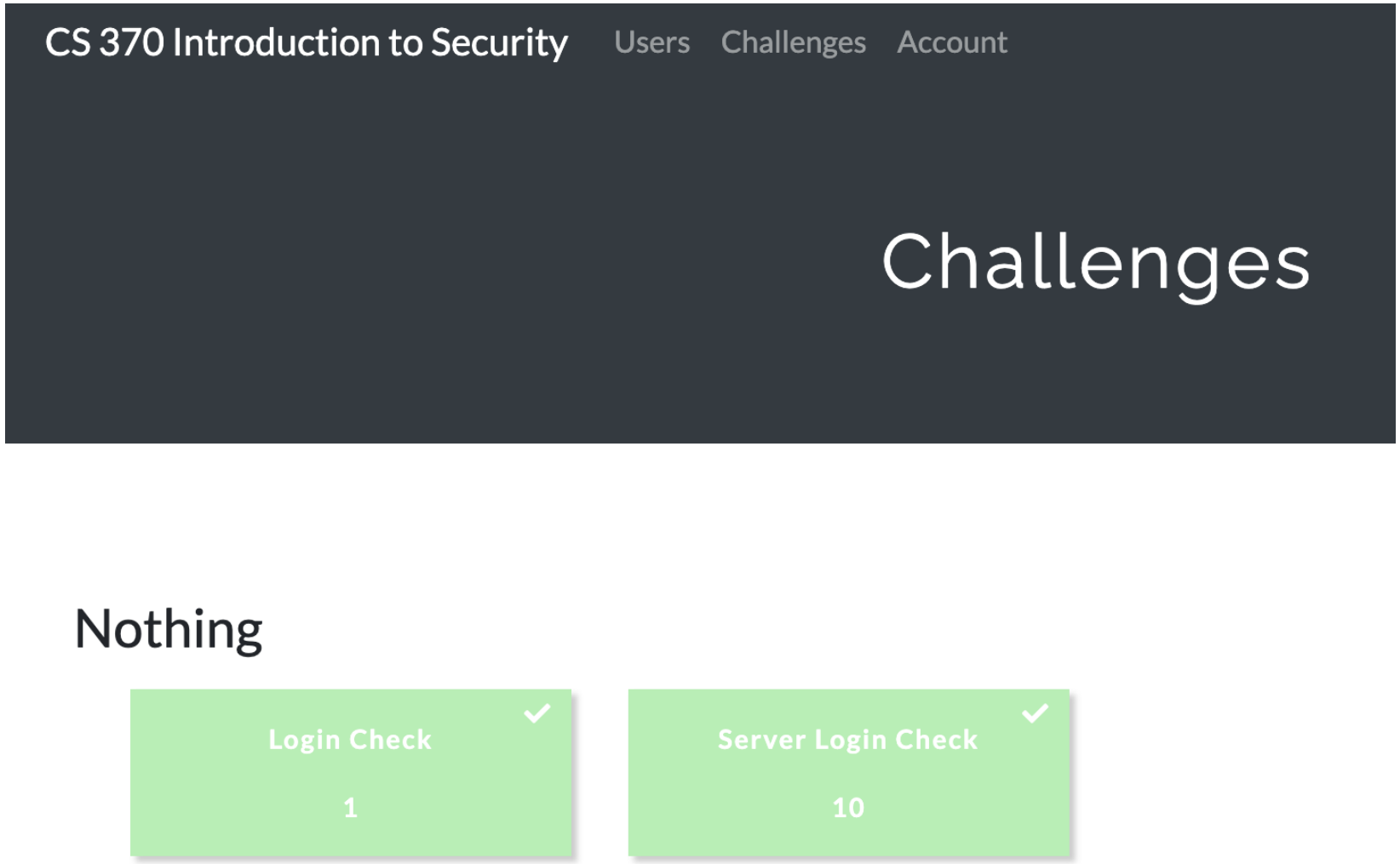
- Four sets
  - Set 3: Authentication and Web Security
    - Practice the use of **password/private-key authentication**
    - **Attack** web server via **SQL injection and parameter injection**
    - **Attack** web service users via **Cross-site Scripting/Request Forgery, etc.**
  - Set 4: Software Security
    - Know how to **find** and **attack** buffer overflow vulnerability
    - Know how to **find** and **attack** logic bugs
    - Apply **static (CodeQL)** and **dynamic (fuzzing)** analysis to programs for finding vulnerabilities…

Micro-Assignments (60%)

- Four sets
  - Set 3: Authentication a
    - Practice the use of **pa**
    - **Attack** web server via
    - **Attack** web service us
  - Set 4: Software Securit
    - Know how to **find** and
    - Know how to **find** and
    - Apply **static (CodeQL)** vulnerabilities…

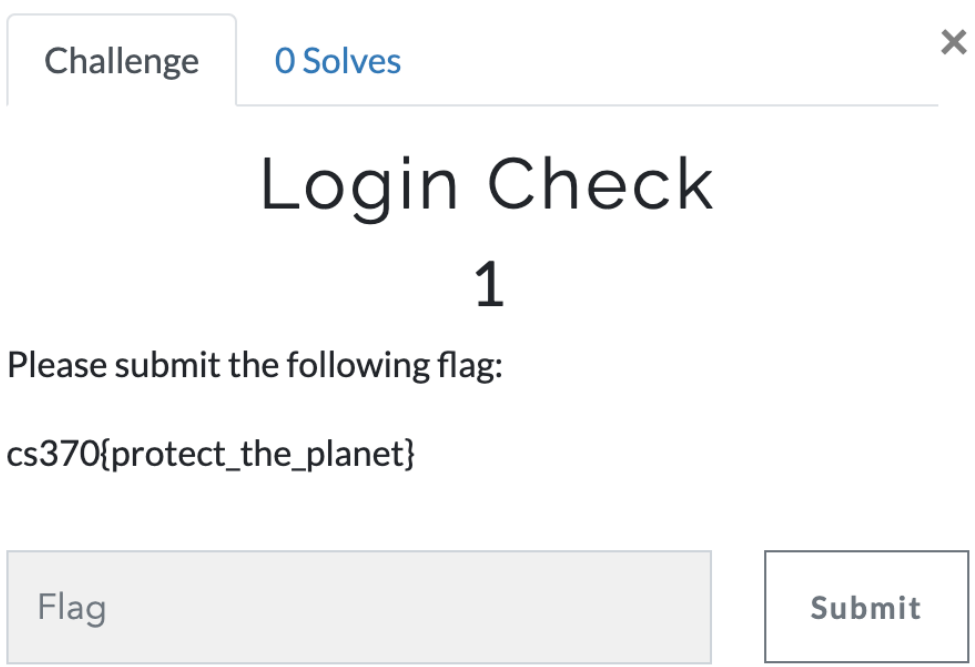
How to Conduct Assignments?

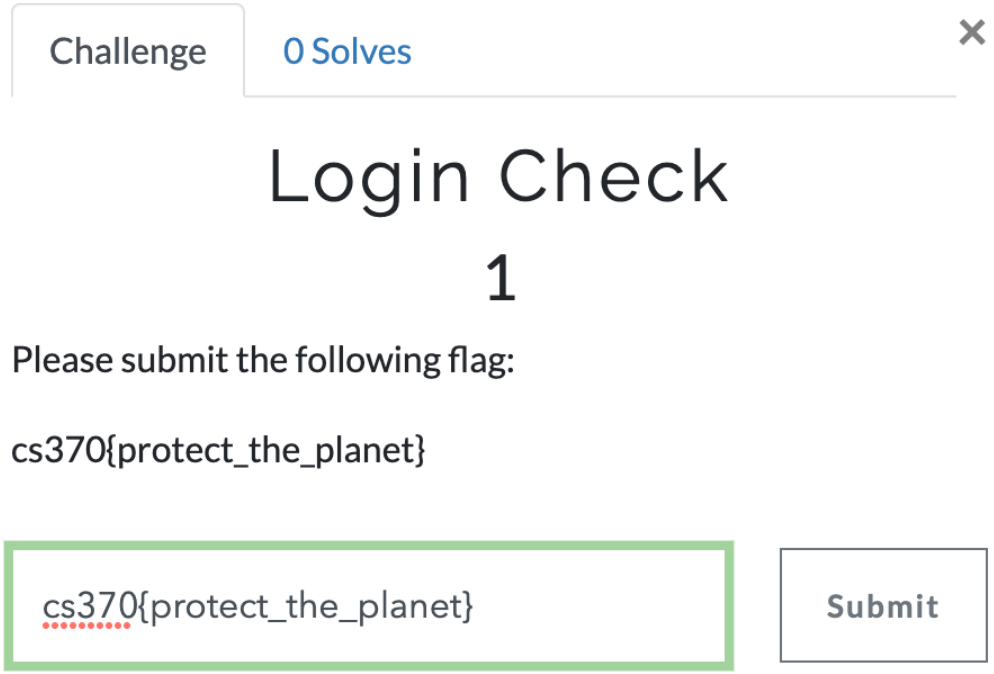
- Scoring System



How to Conduct Assignments?

- Scoring System





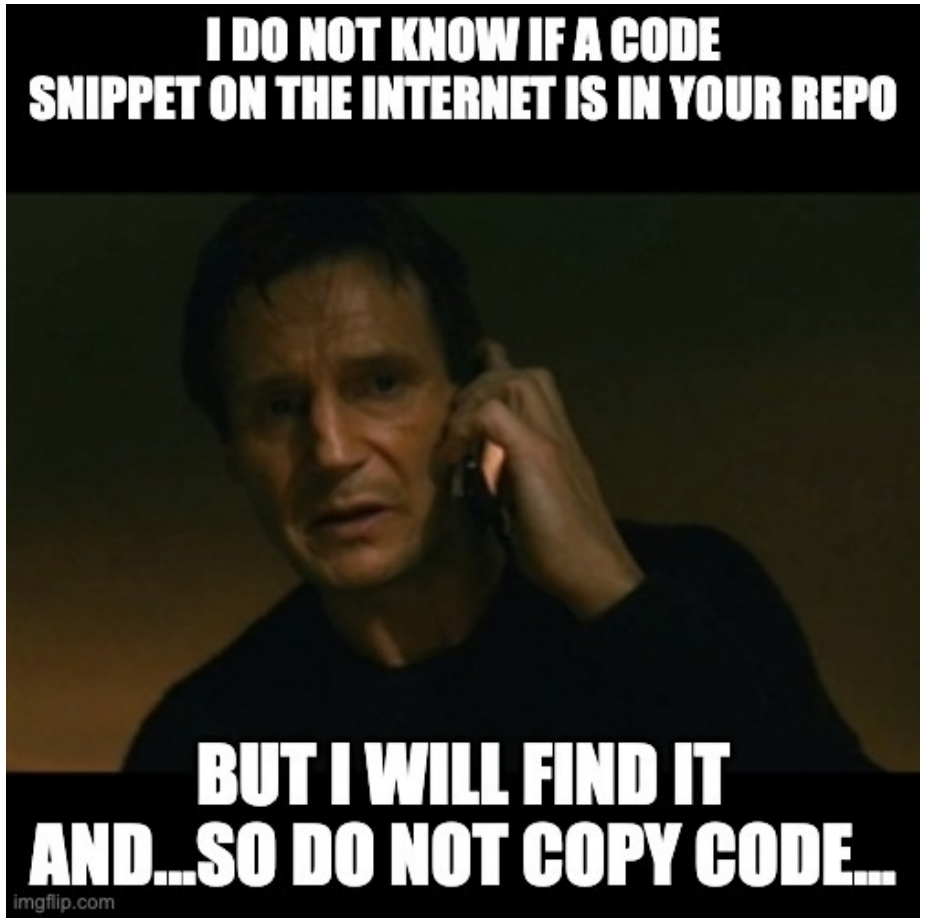
Assignment Rules

- DO NOT SHARE YOUR CODE WITH OTHER STUDENTS
  - **You are encouraged to discuss with others** about the assignments but do not ask/give the code to the others
  - **Do not copy** other students' code or code available in online
  - **Do not publish** your code online

- You will be asked to submit a simple write-up for the assignment
  - Describe how you solve each challenges
  - Mention your collaborators in the write-up
  - **Do not copy** other students' write-up
  - **Do not publish** your write-up online

Lab Rules

- Plagiarism will be punished via the Office of Student Life..
  - E.g., getting F or zero point for the lab assignment that matters with plagiarism…
- Please refer the Code of Student Conduct
  - https://studentlife.oregonstate.edu/studentconduct/academicmisconduct
  - https://studentlife.oregonstate.edu/sites/studentlife.oregonstate.edu/files/edited_code_of_student_conduct.pdf



Due Dates on the Calendar

https://cs370.unexploitable.systems/cal.html

At 2:00 pm of the due date; right before the class starts!

Oct 11
LEC 6: Secure Socket Layer (SSL) and Transportation Layer Security (TLS)
DUE: Cryptography challenges

Oct 18
LEC 8: Quiz 1 prep (cryptography and network security)

Oct 25
LEC 9: User Authentication (password/public-key)
DUE: SSL/TLS and PKI challenges

Nov 1
LEC 11: Web Security Basics (Parameter/SQL injection & directory listing)

Nov 8
LEC 13: Codebreaker Prep 1 (network security)
DUE: Authentication and Web Security challenges

Nov 15
LEC 15: Software Vulnerabilities (Buffer overflow, Logic bugs, etc.)

Nov 22
Quiz 2 (Authentication, Web, and Software Security)

Nov 29
LEC 17: Malware and Stuxnet
DUE: Software Security challenges

Lab Rules – Late Submissions

- If you submit your assignment before the due date, then
  - You will get 100% of credits based on the grading result
- If you submit your assignment within one week after the due date, then
  - You will get 50% of credits based on the grading result
- If you submit your assignment **one week after the due date**, then
  - You will get 0% pts…

Others

- Be active on Discord
- Help each other
- Don’t share the code directly; share concepts & ideas
  - We learn a lot by implementing the concepts with our own hand

Assignment

- Please follow the lab instruction
  - https://cs370.unexploitable.systems/rules.html

- To register yourself on the scoring and the challenge server
  - https://ctf.unexploitable.systems/
  - vm-ctf1.eecs.oregonstate.edu