



# CSC 405

## Computer Security

Alexandros Kapravelos  
akaprav@ncsu.edu

# Who am I?



# Research directions

## Systems & software security



- **Web security & privacy**
  - Evolution of the web and the browser
  - Emerging web threats
  - Web privacy/browser fingerprinting
  - Web behavior
- Software supply chain security
- AI security

# Logistics

- Class website
  - <https://kapravelos.com/teaching/csc405-s25/syllabus/>
- [Piazza](#)
  - Will be adding students to Piazza later this week
- [Panopto](#)
- Discord
  - [HackPack](#) ([website](#))

# Material

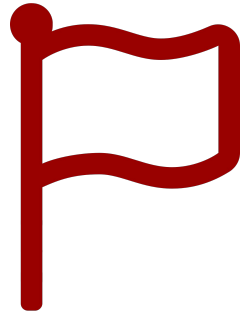
- What material will we be using?
  - Unfortunately, there is no good book on systems security
  - Lecture Slides
  - Related Papers, Readings, and Links
- Useful online books that provide additional information:
  - [The Shellcoder's Handbook: Discovering and Exploiting Security Holes](#)
  - [Hacking, The Art of Exploitation](#)
  - [The Tangled Web: A Guide to Securing Modern Web Applications](#)

# Grading

- What are the requirements to get a grade?
- Homework Assignments - **75%** of grade
  - Shellcode
  - Buffer Overflows
  - Web Security
- Competing in our Capture The Flag competition - **25%** of grade
  - [HackPack CTF](#)

# Capture the Flag

There's a flag...



# Capture the Flag

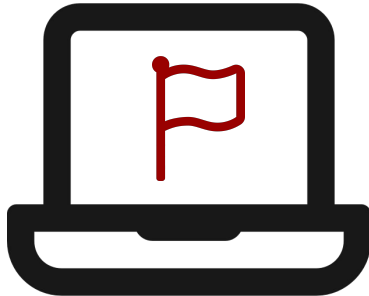
...and you have to capture it.





# Capture the Flag

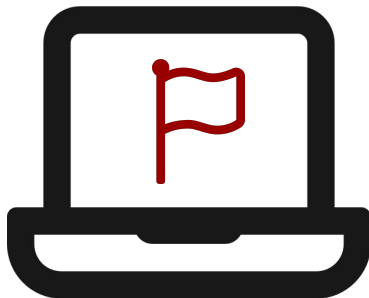
There's a program with a 'flag'



# Capture the Flag

There's a program with a 'flag'

The program has an unidentified vulnerability

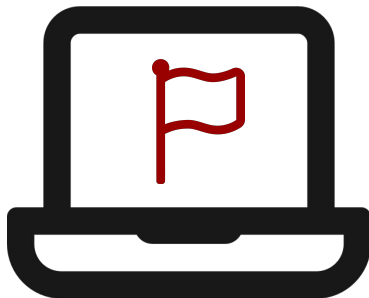


# Capture the Flag

There's a program with a 'flag'

The program has an unidentified vulnerability

You need to exploit the vulnerability to get the flag



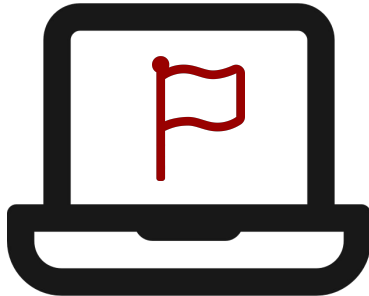
# Capture the Flag

There's a program with a 'flag'

The program has an unidentified vulnerability

You need to exploit the vulnerability to get the flag

The flag is typically a secret string / file



# HackPack CTF

- Capture the Flag Security Competition
- 24 hours of hacking
- **Friday, April 11 2025**
- Competing in the CTF is part of your class
  - For the homework-part you will be able to work on the challenges over the weekend
  - Participation is **mandatory** to the CTF event, if you cannot make it you have to inform me beforehand

# Assignments

- Individual homework assignments
- These are going to be **hard!**
- You are going to implement attacks and defenses
- Discovering a vulnerability is a frustrating, but very rewarding in the end!
  
- The assignments have a unique nature
  - They require some **exploration** from you
  - They are **VERY** different from any assignments you had so far
  - Most of them will have two parts:
    - **Identify** the vulnerability
    - **Exploit** the vulnerability

# Lectures

- In-person
- Streamed on Panopto if you miss the lecture
- Somewhat flipped
  - watch the lecture before you come to class
  - we discuss/solve a security challenge during class
- You will have to watch the lectures and study any related material
- We will use Piazza for any questions

# Topics

Computer Security Basics

Software Security

Web Security



# Goals

Learn how an attacker takes control of a system

Learn to defend and avoid common exploits

Learn how to architect secure systems

# You need to understand

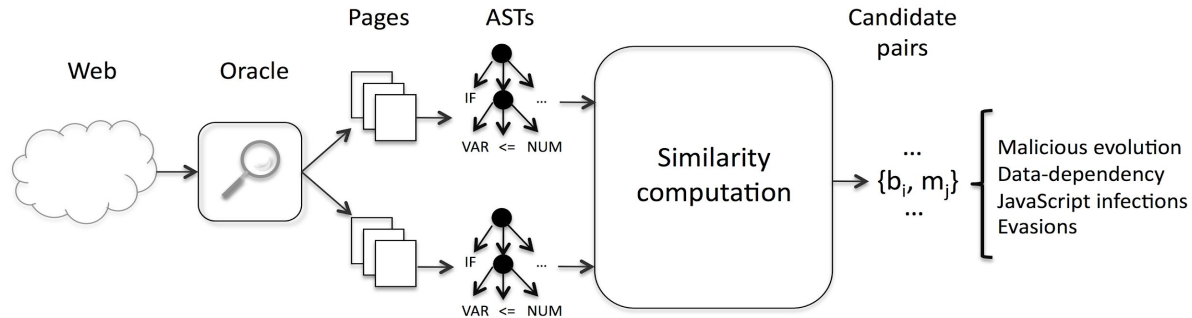
- Networks and Operating Systems
- Basics of systems theory and implementation
  - file systems, distributed systems, networking, operating systems, ...
- You will build stuff. I expect you to:
  - know how to code (in language of your choice\*)
  - I will use mix of pseudocode, Python, Assembly, JavaScript, PHP and C
  - be(come) comfortable with Linux/UNIX

# Readings

- There is a large amount of readings in this course covering various topics:
  - Support the lectures in the course (provide clarity)
  - Augment the lectures and provide a broader exposure to security topics
- **Students are required to go through the readings**
  - Some of the material is **really helpful** in solving the homework assignments

# Cheating

- Cheating is not allowed
- We run tools
  - literally collaborating with Senior Design to make more
- If you cheat you will probably get caught and get a failing grade in the course
- All academic dishonesty incidents will be reported without exception



# Ethics

*With great power comes great responsibility*

- Topics will cover technologies whose abuse may infringe on the rights of others
- When in doubt, please contact us for advice
- Do not undertake any action which could be perceived as technology misuse anywhere and/or under any circumstances unless you have received explicit written permission from the instructor.

# Extra Credit Policy

- Anyone who finds a security vulnerability (on any site/program) during the semester will receive extra credit (bonus points)
- **YOU MUST USE RESPONSIBLE DISCLOSURE**
  - You are responsible for your own actions
  - If you are unsure, come speak with us
  - Do not attack servers you do not own, do not destroy data

questions?