



CSC 405

Computer Security

Adam Gaweda
agaweda@ncsu.edu

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
- LLMs in security

Logistics

- Class website
 - <https://kapravelos.com/teaching/csc405-s24/syllabus/>
- [Piazza](#)
 - Will be adding students to Piazza later this week
- [Panopto](#)
- Discord
 - [HackPack](#) ([website](#))
 - [CSC Hub](#) (unofficial CSC department, not moderated by faculty but *we're watching*)

Material

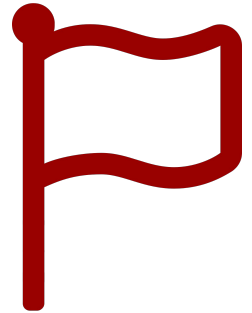
- What material will we be using?
 - Unfortunately, there is no good book on systems security
 - Lecture Slides
 - Related Papers, Readings, and Links
- Useful online books that provide additional information:
 - [The Shellcoder's Handbook: Discovering and Exploiting Security Holes](#)
 - [Hacking, The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

Grading

- What are the requirements to get a grade?
- Homework Assignments - 100% of grade
 - Shellcode
 - Buffer Overflows
 - Web Security
 - [HackPack CTF](#)

Capture the Flag

There's a flag...



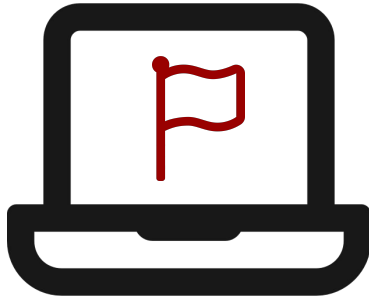
Capture the Flag

...and you have to capture it.



Capture the Flag

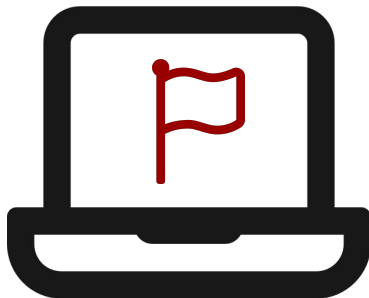
There's a program with a 'flag'



Capture the Flag

There's a program with a 'flag'

The program has an unidentified vulnerability

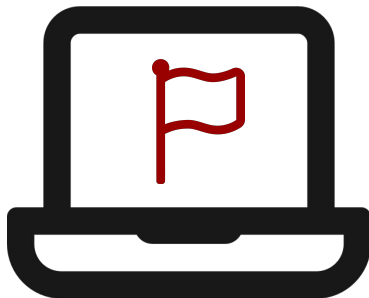


Capture the Flag

There's a program with a 'flag'

The program has an unidentified vulnerability

You need to exploit the vulnerability to get the flag



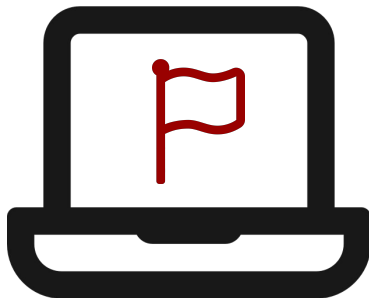
Capture the Flag

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
- **April** (date TBD)
- It will count as one homework assignment
 - 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

 @Phantom0 405 isn't that hard, it's hw-based so you do the work you get the points. Though hw2 was a bit time consuming and low-level so it depends if that's something you might like. 405 is spring-only s

 **Brett** Today at 12:53 PM


How many hours should you expect to take for each homework? Trying to see what to expect


 @Brett How many hours should you expect to take for each homework? Trying to see what to expect

 **naidneeltil** Today at 12:58 PM

pleeeeeeassee don't think if it in hours 😬 most likely your going to work on it, get stuck, post piazza posts, work on it some more, post more piazza posts and slowly work though the problems. there are not very many HW, like 3, then a final CTF game. at *minimum* realistically like 5 days.

keep in mind you get like 2 weeks ish (cant quite remember) in total to do each hw. if you start early, the class becomes waaaay more fun and interesting


 @Brett How many hours should you expect to take for each homework? Trying to see what to expect


 **Phantom0** Today at 1:05 PM

It's hard to put numbers to it but I think like <20h for hw2 and <10h hw{1,2}. The fourth hw is a ctf lol


 **naidneeltil** Today at 1:10 PM


for your own good, *I beg*, don't pull like, a 20 hour marathon two days before to finish a HW. (edited)

 @Blazer yeah

 **naidneeltil** Today at 1:17 PM


Blazer, nearly forgot. if you can work in partners for an assem proj, do so. its better that way (edited)


 @naidneeltil for your own good, *I beg*, don't pull like, a 20 hour marathon two days before to finish a HW. (edited)

 **Phantom0** Today at 1:18 PM


I did try to cram only because I thought I'd be able to speedrun it 💀. Alex was my lord and savior for that class


💀 1

 @PhantomO 405 isn't that hard, it's hw-based so you do the work you get the points. Though hw2 was a bit time consuming and low-level so it depends if that's something you might like. 405 is spring-only s

 **Brett** Today at 12:53 PM


How many hours should you expect to take for each homework? Trying to see what to expect


 @Brett How many hours should you expect to take for each homework? Trying to see what to expect

 **naidneeltil** Today at 12:58 PM

pleeeeeeassee don't think if it in hours 😬 most likely your going to work on it, get stuck, post piazza posts, work on it some more, post more piazza posts and slowly work though the problems. there are not very many HW, like 3, then a final CTF game. at *minimum* realistically like 5 days.

keep in mind you get like 2 weeks ish (cant quite remember) in total to do each hw. if you start early, the class becomes waaaay more fun and interesting


 @Brett How many hours should you expect to take for each homework? Trying to see what to expect


 **PhantomO** Today at 1:05 PM

It's hard to put numbers to it but I think like <20h for hw2 and <10h hw{1,2}. The fourth hw is a ctf lol


 **naidneeltil** Today at 1:10 PM


for your own good, *I beg*, don't pull like, a 20 hour marathon two days before to finish a HW. (edited)

 @Blazer yeah

 **naidneeltil** Today at 1:17 PM

Blazer, nearly forgot. if you can work in partners for an assem proj, do so. its better that way (edited)

 @naidneeltil for your own good, *I beg*, don't pull like, a 20 hour marathon two days before to finish a HW. (edited)

 **PhantomO** Today at 1:18 PM

I did try to cram only because I thought I'd be able to speedrun it 💀. Alex was my lord and savior for that class

💀 1

Alex isn't here this semester

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 → weekly Q&A!

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

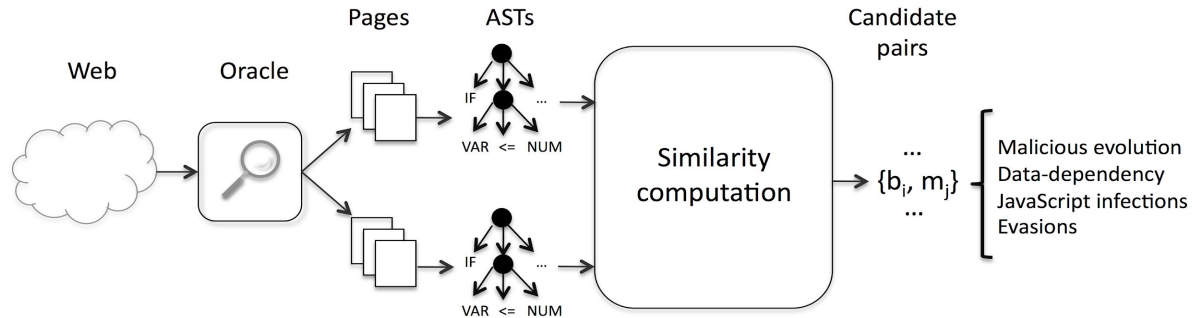
- Networks and Operating Systems
- Basics of systems theory and implementation
 - file systems, distributed systems, networking, operating systems, ...
- You will build stuff. I expect you to:
 - know how to code (in language of your choice*)
 - I will use mix of pseudocode, Python, Assembly, JavaScript,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